Strengthen security with intelligent identity and access management

IBM Security solutions help safeguard user access, boost compliance and mitigate insider threats

Highlights
- Enable business managers to control access for their employees
- Improve user assurance with strong authentication and analytics
- Strengthen identity and access controls (internal and external) for trusted user access beyond boundaries
- Enhance user activity monitoring across security domains with security intelligence

In today’s multi-perimeter world—where users can access your corporate assets from any device, anywhere—it is more important than ever to ensure that online interactions are kept secure, private and compliant. With the growing use of cloud and mobile technologies, the borders of an organization are increasingly blurred. Now, organizations require a people-centric approach to securing access, and this involves more than just managing user provisioning and single sign-on policies. Today’s organizations need to be able to not only control access to sensitive assets, but also monitor the actions of individuals after they have gained access. This way, organizations can identify suspicious behavior—and take action—to help minimize risks and defend against advanced threats.

Identity and access management solutions from IBM® Security are designed to support a people-centric approach to enterprise security and regulatory compliance. By delivering role-based access to the right people at the right time—and then monitoring their use to find anomalies and security gaps—organizations can proactively fix vulnerabilities and help prevent malicious activities in the future.

Secure the extended enterprise

Around the world, organizations are increasing the types of users—including customers, employees, citizens, partners and suppliers—who are allowed to access information across the web, the cloud and federated environments. The need to securely collaborate with business partners, interact with third-party suppliers and online consumers, and support new cloud-based services is making risk-based authentication and access control capabilities even more important. The migration to cloud, social networking and mobile environments requires a scalable, secure identity-based foundation for monitoring and protecting the organization—and its data—against threat, fraud, and internal and external attacks.
With identity and access management solutions from IBM, organizations can take an integrated, intelligent approach to protecting identities across the extended enterprise. IBM solutions include standard capabilities for enabling strong authentication, lifecycle management and single sign-on access, and combine them with next-generation technologies for threat awareness, policy management, and user monitoring and reporting. This way, organizations can centralize access control, while also gaining visibility into “who has access to what” across all resources—both in the cloud and across the infrastructure. At the same time, they can meet business demands for role-appropriate user access, improved customer responsiveness and lower IT costs.

**Key capabilities for integrated security**

IBM Security identity and access management solutions can help protect your corporate assets and information from unauthorized access—and do it without affecting business productivity.

By providing an integrated approach to security that leverages self-service tools and automated recertification, IBM solutions can streamline the delivery of policy-based, compliant user lifecycle management across the organization, while continuously enforcing governance rules and compliance policies. As a result, organizations can move toward sustainable compliance, reduced costs and risks, and enhanced service levels for the multi-perimeter world.

**Support for ongoing security initiatives**

Identity and access management solutions from IBM can both meet the immediate, tactical needs of the organization and also provide a strategic foundation for long-term success. The solutions are designed to empower IT and business leaders to:

- Respond effectively to the rising number of identity-focused attacks
- Safeguard collaboration and access to online resources within cloud, mobile and social environments
- Protect against insider threats and identity fraud while ensuring compliance
- Scale, simplify and accelerate security services for business users and IT staff

**Assess security needs along with business priorities**

By centralizing the management of user profiles and access rights, organizations can protect critical resources from security threats, enforce governance and security policies, and maintain compliance with the latest regulations. Identity and access management projects can gain better executive collaboration when they are aligned with an organization's business priorities. They can also benefit from a careful assessment of the organization's security challenges, access control policies and practices, and regulatory climate. IBM recommends that organizations keep these factors in mind when determining investment priorities and requirements for identity and access management, and then use a formal assessment to develop the blueprint for implementation.

The following sections describe ways that IBM Security offerings help organizations centrally manage and automate identity lifecycle management, access control and security analytics across the enterprise, from mainframe to workstation.

**Enable business managers to control access**

IBM Security Identity Manager can help organizations implement key identity management capabilities, such as user provisioning, self-service, privileged-user management and security intelligence for end-to-end user visibility. It can automate the management of user roles, identities and access rights throughout the entire user lifecycle. IBM Security Identity Manager includes embedded role lifecycle management capabilities, which can help streamline the role structure approval process and reduce errors when validating access with the business. It also provides direct access to enhanced reporting and analytic capabilities.
Working with existing platforms—across distributed and mainframe environments—IBM Security Identity Manager helps administrators to centralize user definition and user service provisioning to help minimize errors and inconsistencies. When integrated with other IBM identity and access management solutions and the broader IBM Security portfolio, it provides a strong foundation for securing today’s dynamic environments.

IBM Security Identity Manager comes with Identity Service Center, an easy-to-use, intuitive user interface that can help business managers request access rights for their employees. These self-service capabilities can help business managers make intelligent access decisions for their employees while saving valuable time for IT staff.

In addition, organizations need a way to track the use of shared and privileged credentials to help protect against unauthorized access. IBM Security Privileged Identity Manager can help reduce the risk of insider threats by centralizing the management of privileged and shared identities and reporting on the activities of these users. Organizations can 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.

**Strengthen identity and access controls (internal and external)**

IBM also offers leading access management solutions that can help organizations block external attacks, safeguard user access in cloud and mobile environments, and prevent security breaches. IBM Security access management solutions help organizations protect critical IT resources from unauthorized access and comply with security regulations. With convenient single sign-on and context-based access control, these solutions can help proactively enforce access policies to prevent threats and identity fraud across cloud, social and mobile collaboration channels. In addition, IBM solutions help support compliance by maintaining centralized audit trails for access requests and preventing unauthorized access—all while enabling administrators and users to be more productive.

Available as physical or virtual appliances, IBM Security access management solutions provide a single point of authorization for web, cloud-based and enterprise applications, helping organizations to overcome the difficulties of implementing security policies across a wide range of web and application resources. For example, IBM Security Access Manager for Mobile provides risk-based capabilities to help protect access to an organization’s information assets via mobile devices. With risk-based access, each transaction is assessed using static and contextual attributes to calculate the risk. This risk assessment determines whether a user’s request to access information should be permitted, denied or permitted with some further authentication. As a result, organizations can consistently provide employees, partners, suppliers and customers with secure access to the information and services they need.

**Improve user assurance with strong authentication**

IBM Security access management solutions also provide users with streamlined, single sign-on access to protected resources—even on mobile devices—which also helps strengthen enterprise security. Users only need to keep track of a single identity and password. This not only simplifies the user experience, it also helps reduce the incidence of lost passwords—and the resulting loss of productivity for users and IT staff—and minimize security vulnerabilities associated with passwords that are written down in unsecured locations. IBM Security Access Manager for Enterprise Single Sign-On also supports a wide variety of strong authentication devices including smart cards, tokens, badges and biometric devices.
By centralizing user authentication and authorization with IBM solutions, organizations can help ensure that users are who they claim to be and enforce access policies once users have been authenticated. Plus, they can leverage secure session management for online portal and business initiatives to help safeguard transactions and sensitive data.

**Enhance user activity monitoring across security domains**

The integrated portfolio of IBM Security identity and access management solutions can help centralize user lifecycle management across the enterprise, allowing for consistent execution of security policies across multiple applications and all categories of users, including privileged and mobile. The portfolio also provides built-in IBM Cognos®-based audit reporting and real-time insider fraud detection with integrated security intelligence.

IBM Security Identity and Access Assurance is an integrated software solution for protecting an organization’s business and IT assets from unauthorized access and exposure. This IBM solution helps strengthen security with automated identity 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 solution includes built-in reporting and log management functionality from IBM Security QRadar® Log Manager to automatically capture and centrally collate user access activities, highlighting abnormal or out-of-policy activity so the issues can be addressed and corrected.

IBM Security identity and access management solutions integrate with IBM Security QRadar, providing the user activity and identity information that QRadar correlates with other security data to help detect and remediate malicious behavior.
IBM Security QRadar solutions provide contextual and actionable surveillance across the entire IT infrastructure, reducing thousands of security events into a manageable list of suspected offenses to help distinguish real threats from false positives. By integrating QRadar with IBM Security identity and access management solutions, organizations can:

- Control user privileges via a centralized access control policy management platform
- Identify internal threats by increasing visibility into who—and not just what—is accessing valuable networked assets
- Improve compliance reporting by tracking the use of user rights and administrative privileges

**Why IBM?**

Protecting user access in mobile, cloud and online environments—or managing dynamic user groups in complex organizational structures—requires a more integrated, intelligent approach to identity and access management. IBM Security solutions are trusted by organizations worldwide for end-to-end user identity and access management, strengthening security without restricting the timely access to critical resources. They provide visibility and enforcement of user access to data, applications and infrastructure.

**For more information**

To learn more about IBM Security solutions for identity and access management, please contact your IBM representative or IBM Business Partner, or visit: [ibm.com/security](http://ibm.com/security)

**About IBM Security solutions**

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 and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.
© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2014

IBM, the IBM logo, ibm.com, Cognos, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

GMS10332-USEN-02