Prevent advanced insider threats with IBM Security solutions

Manage privileged identity activity, increase visibility, protect against unauthorized access

Highlights

- Help secure user access across the enterprise with strong authentication controls and automated single sign-on (SSO) capabilities
- Ensure individual accountability with fine-grained logging and reporting of privileged user access activities
- Streamline administration of privileged identities throughout the user lifecycle to reduce risk and ensure compliance
- Enable trusted access for privileged users, but verify their actions with optional session recording and security intelligence
- Identify anomalous user behavior using identity information from across the environment
- Support compliance with government and security regulations

Are you confident that only the right people are getting access to your sensitive business assets? Organizations have to be concerned about privileged insiders compromising security—and about outsiders posing as authorized users but who really aren't. Putting effective defenses into place, as a result, requires organizations to look both ways. They need to safeguard privileged accounts inside the enterprise at the same time as they monitor their inside and outside activities—because no matter where it originates, a breach can significantly damage an organization's reputation and bottom line.

An international telecommunications company, for example, was using spreadsheets to manually track IDs for 250 privileged users—a system that was both unreliable and insecure. Why the danger? Because privileged users, whether they have malicious intent or are simply not being vigilant, require close attention. And demonstrating oversight of privileged user entitlements and access activities is often required to comply with government security regulations.

But even when internal and external privileged users, their IDs, their access and their behaviors are effectively managed, they can still put an organization at risk. If privileged users themselves aren't also kept safe from attack, a third party can steal their credentials and use that information to breach the security systems.

In the case of the telecommunications company, the security team recognized the danger, abandoned its spreadsheets and deployed comprehensive identity and access management solutions from IBM. This enabled increased security by restricting user visibility of sensitive login credentials, and provided central, auditable control of privileged IDs.

To help prevent advanced insider threats and identity-related fraud, IBM® Security provides solutions for controlling and auditing shared and privileged identity activity, protecting content against inappropriate access, and correlating monitored user activity with detected anomalies.

Controlling and auditing shared and privileged identity activity

In many organizations, privileged identity management may be incomplete, complicated to administer or noncompliant with regulations. While only trusted employees should have access to sensitive data, verification of who qualifies as a trusted employee must be conducted regularly. A software company, for example, needed to control and audit its 86 privileged identities and provide accountability and security for its privileged shared IDs. IBM Security solutions provided the capabilities it needed, with access approvals required for changes to privileged identities.

The automated privileged identity management capabilities of IBM Security Privileged Identity Manager gave the company the ability to eliminate shared passwords while ensuring compliance and audit support. Designed to streamline the management and monitoring of privileged and shared accounts, the solution provides strong authentication controls and SSO capabilities for high-risk account access. With the ability to record and replay user sessions, it can address both regulatory and privacy requirements to support audits and compliance.

Mitigating credential theft and account takeovers

Insider threats are often difficult to identify and eradicate because they manifest as authorized users performing legitimate functions. What's more, if a user with privileged access is the victim of a successful attack, then the attacker can end up with the user's credentials. Facing the possibility of such attacks, a company in India needed centralized, secure management to audit privileged identities and track access to resources. IBM Security solutions gave it the ability to help ensure security and simplify user activities by automatically providing systems with credentials.

IBM Security Privileged Identity Manager gave the company strong authentication controls and SSO capabilities for high-risk account access. Additionally, by managing the creation, modification and termination of user privileges, IBM Security Identity Manager helps establish and maintain appropriate credentials using role-based policies to identify abuse. IBM Trusteer™ application protection technology helps to prevent malware from tampering with applications, while sending alerts of abnormal behavior.

IBM Security solutions help fight advanced insider threats by managing privileged users' identities, tracking and reporting on their access activities, and recertifying their rights to access resources:

- **IBM Security Privileged Identity Manager—Secures, automates and tracks privileged IDs and sensitive data access to protect enterprise resources; delivers effective privileged identity control with a secure credential check out, SSO and optional session recording to support compliance reporting requirements**
- **IBM Security Access Manager for Enterprise Single Sign-On—Provides visibility into user activity, control over user access, and automation of sign-on processes; it tracks and reports on user access activities with session management and fine-grained application audit logs**
- **IBM Security QRadar® SIEM—Collects and analyzes identity data to improve visibility into how access is being utilized; QRadar analytics and security intelligence can help uncover identity anomalies and inappropriate actions**

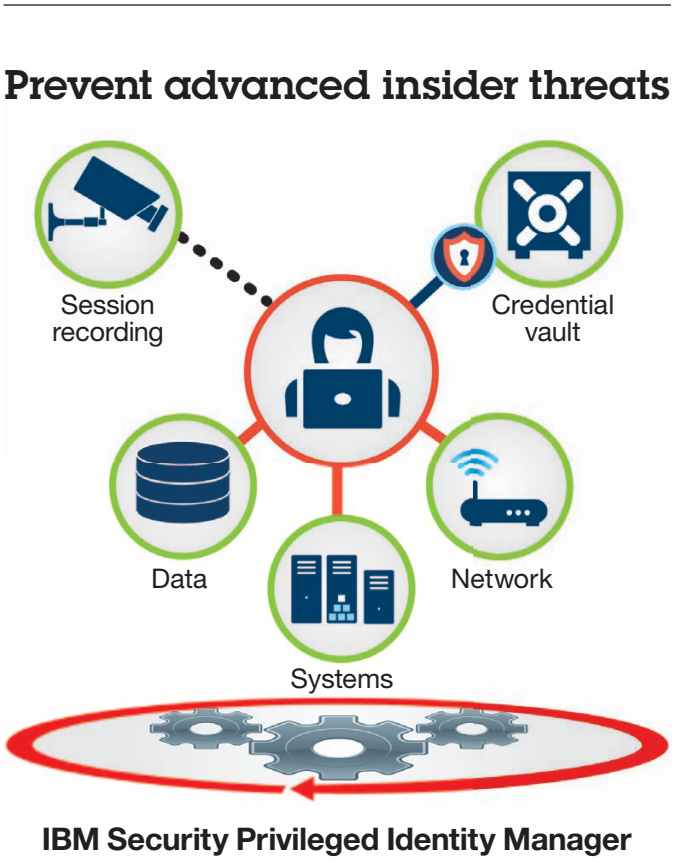
Securing access and protecting content from unauthorized use

With exponential growth of employees and agents, a life insurer in India was facing numerous challenges in account management and policy enforcement. In particular, it experienced critical issues in its identity and access-management environment, which made the environment unstable. The company sought a robust solution that would help centralize the monitoring and management of user identity and access while protecting access to its applications.

IBM Security Access Manager for Enterprise Single Sign-On allowed the company to centralize management and enforce user-authentication, authorization and audit processes while lowering account-management costs and security exposure. Further, the company reduced costs through centralized management of user accounts and improved user productivity through convenient SSO to customer accounts.

Correlating monitored data activity with detected anomalies

A major Mexican bank struggled to analyze security logs in a timely and efficient manner, which left it vulnerable to security incidents from internal and external actions. In addition, the user-authentication solution it used for customer online applications failed to meet security requirements of national regulatory bodies. IBM Security solutions gave the bank improved ability to analyze logs, reduce risk and help ensure secure access with SSO capabilities for users and management of access privileges from a centralized console.



IBM Security Privileged Identity Manager controls and helps protect the use of administrative IDs, monitors and records access sessions, and employs analytics and security intelligence to discover anomalies and inappropriate actions.

Using IBM Security Privileged Identity Manager and the IBM Security Identity and Access Assurance solution bundle, the bank could ensure compliance and audit support with the ability to record and replay user sessions. Using IBM Security QRadar solutions, it can automatically identify suspicious user activity patterns, so the security team can shut down account takeovers before they do damage.

Why IBM?

IBM Security solutions are trusted by organizations worldwide to help administer and secure user access to resources, monitor for abnormal behavior and maintain compliance with regulatory mandates. In response to this need, IBM Security solutions take a holistic approach to security requirements related to identity fraud and insider threats to help organizations move from reactive responses to proactive action.

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

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.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2014

Please Recycle

WGS03021-USEN-01