IBM Security Privileged Identity Manager helps prevent insider threats

Securely provision, manage, automate and track privileged access to critical enterprise resources

Highlights

- Centrally manage privileged user identities and entitlements to mitigate insider threats
- Simplify privileged identity management functions with an intuitive user interface
- Request, approve and revalidate privileged access to reduce risk and improve compliance
- Helps protect access to enterprise resources with automated password management
- Provide accountability with session recording/replay support and usage tracking of shared IDs
- Help reduce total cost of ownership (TCO) and speed time to value with a virtual appliance deployment option and new administrative tools

Within virtually every organization, there is a set of privileged users—IT administrators, high-level executives and others—who have elevated access to sensitive IT resources across systems, applications and platforms. And while their privileged IDs are usually shared among a limited pool of users, they can cause major accountability and compliance issues, increasing the risk for sabotage and data theft. From inadvertent mistakes to intentional malfeasance, the misuse of these privileged IDs can cause serious damage.

In fact, the insider threat problem has become so pervasive, it generated a response from the US White House. In November 2012, the White House issued a presidential memorandum that outlines the minimum elements of effective insider threat programs.[1] Recommendations include developing the capability to gather, integrate, and centrally analyze and respond to key threat-related information, as well as monitoring employee use of protected networks.[1] By monitoring employee-use patterns, organizations can identify and thwart insider threats.

Organizations don't need to leave themselves vulnerable to insider threats. IBM® Security Privileged Identity Manager delivers a single solution for securing, automating and tracking the use of privileged IDs. By centralizing the management of privileged identities, Security Privileged Identity Manager 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.

The need to manage and track privileged users

The trends toward data center consolidation, outsourcing, cloud computing and virtualization are increasing the overall number of privileged users within today's IT infrastructures. When doing business with outside service providers, organizations also need to protect their information from misuse by vendors and to maintain an effective governance posture. Protecting corporate IT resources from these "super users" is more important than ever. Current and emerging government regulations outline the technical accountability issues with which organizations must comply, or face financial and criminal penalties. Industry standards also require more fine-grained control of the activities and accesses of privileged users. Maintaining regulatory compliance while also guarding against insider security breaches has resulted in a compelling business need to securely manage and track privileged user identities.

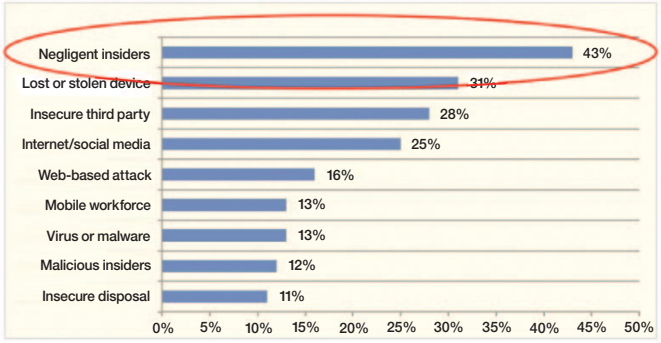
The growing threat of the trusted insider

Who can be trusted with administrative accounts and privileges? Today's organizations are faced with the growing challenge of protecting data and applications from security breaches. These breaches are expensive to resolve, can cause noncompliance with industry standards and government regulations, and can result in costly damages to corporate reputations. Consequently, organizations invest in security technologies and policies to keep the "bad guys" out, often without realizing that the greater threat may be in-house. The security threat posed by the privileged insider can be more dangerous than that of the most determined outside hacker.

Security breaches by trusted insiders are increasing, costly and largely caused by the misuse of privileged user IDs. Disgruntled employees can be adept at maneuvering around access controls to exploit points of weakness.

While malicious insiders are commonly blamed for internal security breaches, many of the breaches are caused by simple negligence. In a recent survey of C-level executives, negligent insiders were identified as the greatest threat to sensitive data.[2] The negligence can range from writing down administrative passwords, to neglecting to deprovision a departing employee's privileged user profile, to forgetting to log off at a shared workstation—typical scenarios that open the door for an unauthorized user to access and exploit sensitive data and client records.

The source of greatest risk to sensitive data



Source: IBM and Ponemon Survey of 265 C-Level Executives, February 2012. "The Source of Greatest Risk to Sensitive Data"

The solution: Privileged identity management

Traditionally, IT administrators have been given their own individual accounts with privileged access to every system. But in the age of consolidation, virtualization and cloud computing, the number of unique IDs needed for each server can escalate exponentially. The typical organization has to manage tens of thousands of privileged passwords, along with the overhead associated with provisioning, deprovisioning and recertifying large numbers of privileged users. While the risks and costs of maintaining these accounts continue to increase, productivity across the organization can suffer dramatically.

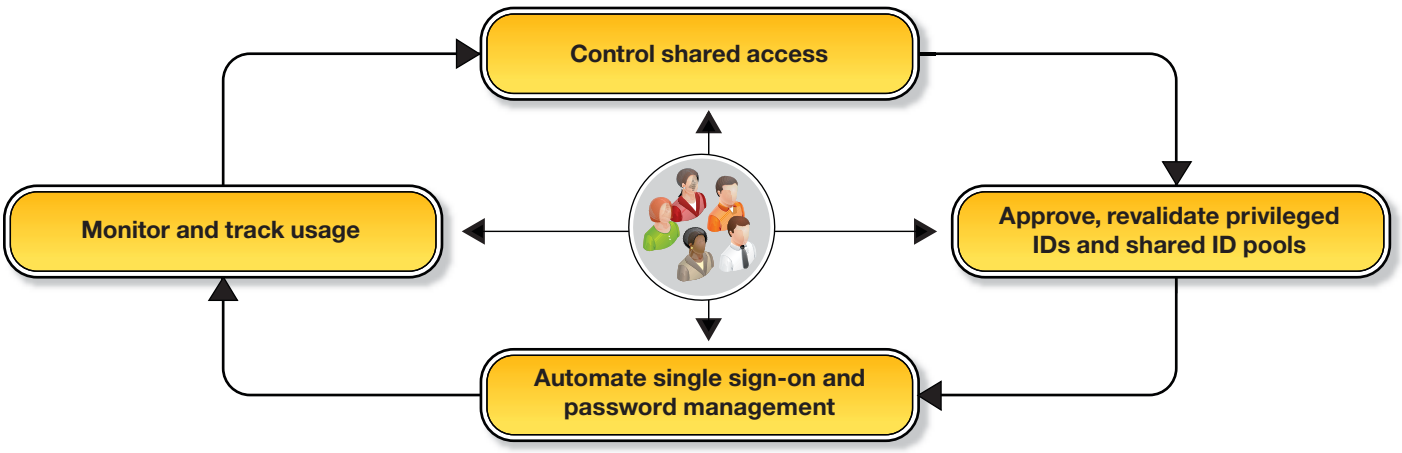
Simply sharing a single privileged ID does not address the problems, either. Deciding how to store and communicate a shared password can be an issue, often leaving an organization's most sensitive privileged accounts as the most vulnerable. When employees terminate employment or change jobs within an organization, a shared password has to be immediately changed. In addition, the anonymity provided by a shared ID makes it difficult to tie a security breach back to a specific individual, guaranteeing problems with regulatory compliance.

Organizations must therefore put into place tools and processes that enable them to manage privileged access and reduce the insider threats to enterprise security, including:

- Secure provisioning of privileged user accounts
- Strong password management and strong authentication policies
- Fine-grained activity logging for shared and privileged identities
- Automated processes that improve productivity while strengthening security

Security Privileged Identity Manager provides complete identity management and enterprise single sign-on capabilities for privileged users, mitigating insider threats by securing and tracking the use of privileged identities. Building upon the foundational technologies of IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On, this solution moves beyond traditional approaches for managing privileged users. Security Privileged Identity Manager can centrally manage and audit a pool of privileged user IDs, which can be checked in and checked out by authorized people when needed. This capability enables organizations to effectively control shared access, manage privileged accounts, track usage and automate password management.

Privileged identity management lifecycle



IBM provides a comprehensive solution for securely managing privileged identity use.

Security Privileged Identity Manager is a comprehensive solution for managing the privileged identity lifecycle. The solution automates the single sign-on and check-in and check-out processes to help simplify use and reduce costs. Security Privileged Identity Manager also provides comprehensive tracking and reporting to enhance accountability and compliance by capturing both *how* a privileged ID was used and what a user did with that privileged ID.

Control shared access to sensitive user IDs

Security Privileged Identity Manager enables shared access among a predefined group of users and provides single sign-on for each user in the group to a designated shared account, even as the password is updated. The solution can be configured to enforce strict check-in and check-out of a pool of shared accounts to ensure accountability. Key features include:

- An encrypted secure vault for securely storing privileged user credentials
- Shared identity services that allow users to request access to a privileged account
- Extended self-service interface for users to optionally check out credentials, view passwords and check in credentials
- Timed auto check-in that gives users a limited time to use a privileged identity
- Password reset that can be configured to run at every check-in, ensuring that passwords aren't compromised

Request, approve and revalidate privileged access

Through the use of roles, accounts and access permissions, Security Privileged Identity Manager helps automate the creation, modification and termination of user privileges throughout the entire user lifecycle. As part of its identity management capabilities, the solution features the Identity Service Center, an intuitive user interface that can help business managers request access rights—including accounts, roles and group membership—for their employees, including privileged users. The roles-based control helps streamline administration of privileged identities to reduce risk and ensure compliance. Organizations can:

- Secure access via a hierarchical role structure
- Enable self-service requests to improve productivity
- Add, remove or change privileged access from a central location
- Automate approvals and recertifications to eliminate costly manual processes
- Create audit trails with detailed reports

Track usage of shared identities

With its fine-grained logging of user activity, Security Privileged Identity Manager enables organizations to demonstrate compliance with government security regulations. Privileged identities are checked out exclusively by individual users—and all steps of authentication and privileged account actions are recorded in a detailed audit trail. This helps organizations ensure individual accountability.

An optional Privileged Session Recorder tool provides full-session auditing, recording and replays of privileged-user activities, delivering forensics and reporting on privileged users to help improve security compliance. With the Privileged Session Recorder tool, each user's session activity, including typed characters and mouse clicks, is recorded, stored and made available for forensics and compliance reviews. Auditors and managers can subsequently search and replay these recordings for governance or troubleshooting purposes.

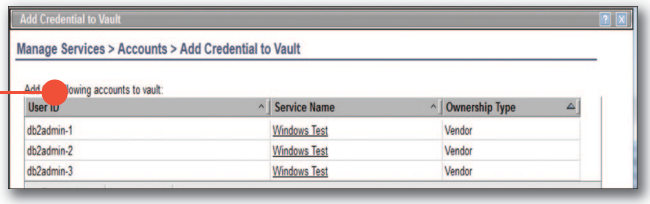
Automate password management

Security Privileged Identity Manager supports single sign-on access with strong authentication that hides the current password from the end user, delivering an additional level of assurance. With automated password management, organizations can:

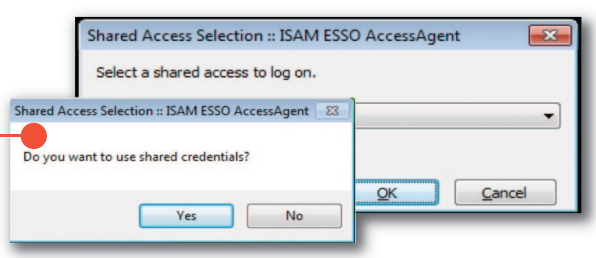
- Automate the check-out of IDs
- Hide passwords from the requesting employee
- Require password resets after use and upon check-in to eliminate password theft and reuse outside the governance structure

Controlling privileged IDs: How it works

Configure privileged account.

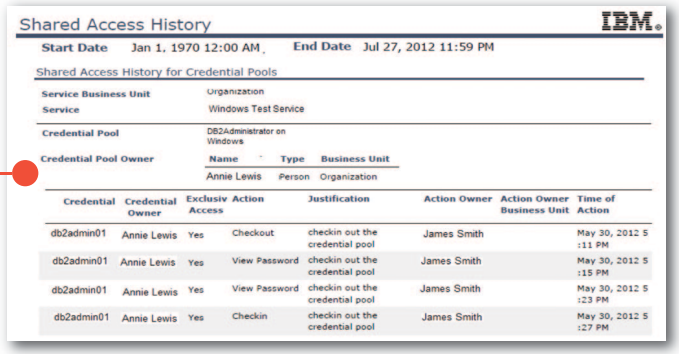


User's credential is automatically **checked out** of the vault and used to **log user into** privileged account. Credential is automatically checked in to vault upon logout.



Administrator ID

User activity is **logged.**



IBM Security Privileged Identity Manager supports privileged identity management with a secure credentials vault and automated single sign-on capabilities.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity and access management. With IBM solutions, organizations can safeguard, automate and track the use of privileged identities; improve IT governance; avoid the high cost of identity proliferation; and increase security across the entire enterprise. IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. These products build on the threat intelligence expertise of the IBM X-Force® research and development team to provide a preemptive approach to security.

For more information

To learn more about IBM Security Privileged Identity Manager, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2013

[1] The White House, Office of the Press Secretary, "Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012. http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

[2] IBM and the Ponemon Institute, "The Source of the Greatest Risk to Sensitive Data," *Survey of 265 C-Level Executives*, February 2012.

Please Recycle

WGS03005-USEN-01