IBM Software
Thought Leadership White Paper

October 2012

Avoiding insider threats to enterprise security

Protect privileged user identities across complex IT environments—even in the cloud

IBM

Contents

Introduction

Today's organizations are highly vulnerable to security threats related to privileged identities—that is, the accounts of system administrators, database managers and others with elevated access to critical IT resources. Because of the overarching access of these users, their privileged identities have extraordinary abilities to control and exploit an organization's data, applications and endpoints. For the sake of security, organizations must maintain tight controls over who they grant privileged identity status to—and what they do with those privileges. Administrators need to effectively manage the provisioning and deprovisioning process for privileged users, including separation-of-duty checks, and implement policy-based workflows and authorization processes for granting and updating users' credentials in a timely manner. These familiar identity and access management activities are made more critical due to the elevated risk of abuse through privileged access. However, the process is complicated by the fact that privileged accounts are typically shared between multiple users, often eliminating individual accountability and exposing the accounts to potential security violations. Shared credentials are easily violated because they can't be easily revoked after a privileged user changes roles or leaves the organization. Ideally, organizations need to be able to closely guard and easily change these shared credentials.

Former or disgruntled employees are an obvious source of security breaches, as are careless users who inadvertently leave their systems open to attack. But external threats also come into play. On today's smarter planet, which is increasingly interconnected, organizations are now at risk from security gaps from their cloud service providers, outsourcing partners and across other third-party environments. Poor password management, for example, may enable hackers to break into a privileged user's account, providing them unrestricted access to the account's administrative credentials and resources. A compromised privileged account can cause data leakage, corrupted records or applications, even operational shutdowns.

More than ever, successful business operations hinge on securely and efficiently managing access by privileged users. Data theft related to compromised accounts and corporate sabotage can damage an organization's reputation as well as its bottom line. In addition, organizations must be vigilant about complying with the latest government regulations for IT security—or face significant financial and criminal penalties. Industry standards have become more specific in regards to data security and the privileged accounts that can access data.

IBM® Security Privileged Identity Manager helps organizations to securely manage and track the activities of privileged users, thereby reducing the risk of breaches, improving compliance and ensuring accountability. Providing a complete privileged identity management solution in a single, integrated offering, Security Privileged Identity Manager enables privileged users to implement the same solution for both their privileged and standard IDs—with just one user interface to learn and one identity and access management (IAM) system to maintain.

And IT administrators can easily integrate Security Privileged Identity Manager into their existing infrastructure for improved efficiencies and cost savings. This white paper explains how Security Privileged Identity Manager provides enhanced security across various IT environments by centralizing and controlling the use of privileged identities.

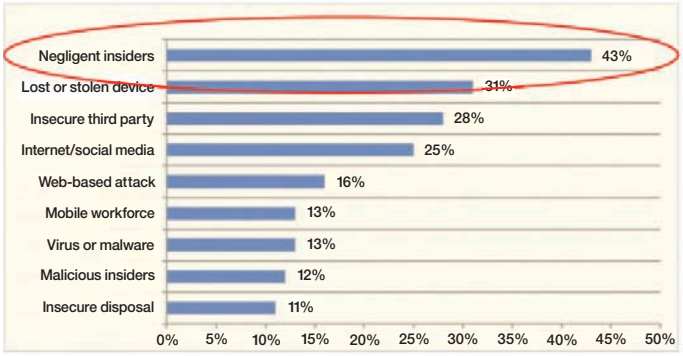
Securing the modern enterprise

Insider attacks are becoming more prevalent. In fact, according to the Kroll Annual Global Fraud Report, a survey that polled more than 1,200 senior executives worldwide, the number of frauds committed by insiders rose from 55 percent to 60 percent in a one-year period.[1] From network administrators to high-level executives, organizations have a number of privileged users who require elevated access to business-critical resources. Because these "super users" routinely access a variety of IT systems, applications and data to perform their jobs, they can be a substantial threat to an organization's information integrity and data privacy.

With the rise of social media, cloud computing and mobile collaboration, insiders have more ways to pass sensitive information to unauthorized outsiders with less chance of discovery. And the definition of a "trusted insider" has expanded to include employees, contractors and consultants, as well as business partners and service providers. Even the unintentional actions of these trusted insiders can result in costly consequences.

Sometimes it is insider negligence, rather than malicious behavior, that causes enterprise security breaches. Examples include writing down administrative passwords, forgetting to deprovision a departing employee's privileged user profile and 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. Whatever the motive, organizations must address any and all threats to sensitive data and applications.

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"

Controlling privileged access to cloud-based resources

With ongoing pressure to increase productivity and decrease costs, IT organizations continue to seek out new ways to more efficiently manage and outsource IT resources. These changes include tighter integration with business partners, increased levels of outsourcing, and leveraging virtualization and cloud computing. In fact, the prevalence of cloud computing has dramatically changed the security landscape. The cloud extends services, applications and resources to a broad user base that may include employees, customers and partners. The importance of monitoring and regulating privileged users only increases with cloud and virtualized environments, because organizations no longer control the infrastructure and have limited visibility inside clouds. Organizations should implement policies that can manage privileged accounts regardless of where they reside and that include the ability to enforce policies, even with cloud providers.

IAM tools that can monitor, report and proactively reduce user security violations are essential. An automated IAM solution can streamline the setup and enforcement of security policies across the enterprise—and into the cloud. This helps an organization make the most of limited resources and tight budgets by using a single IT security infrastructure, versus two separate sets of applications. However, even with an IAM solution, the traditional method of managing privileged identities can be costly and unwieldy.

Managing the explosion of privileged identities

Traditionally, organizations have used two approaches to manage privileged identities: 1) Creating a set of shared accounts that all privileged users can access when needed; and 2) Giving IT administrators their own individual accounts with privileged access to every application or system they support. The first approach lacks accountability and is easily breached, while the second approach is very complex and hard to scale. With the emergence of global delivery centers, blade servers, virtualization and cloud computing, the total number of unique IDs needed for each server has skyrocketed. The typical organization now has to manage tens of thousands of privileged passwords. While the risks and costs of maintaining these accounts continue to increase, productivity across the organization can suffer dramatically.

Simply sharing privileged ID credentials does not address the problems, either, leaving an organization's most sensitive privileged accounts as the most vulnerable. When employees leave or change jobs, a shared password has to be immediately changed. In addition, the anonymity provided by a shared ID makes it difficult to tie an action or security breach back to a specific individual, guaranteeing problems with regulatory compliance.

Business leaders are left to wonder: How do we set up and maintain appropriate user access privileges for our sensitive resources? Do a privileged user's entitlements map correctly to the role he/she has within the organization? How can we enforce and demonstrate compliance with industry regulations and business policies that protect data privacy and integrity? How do we implement a reliable way to quickly identify, track and stop suspicious activities and unauthorized behaviors before they spiral out of control?

A successful privileged identity management solution addresses these issues and is an integral part of a complete identity and access management framework, not a standalone vault solution. It should include the following capabilities:

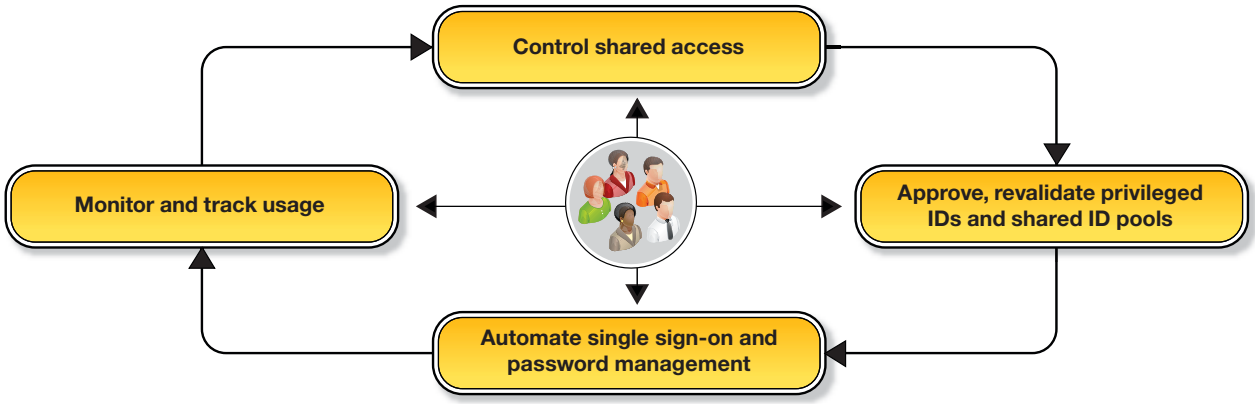
- Centralized management of the entire privileged identity lifecycle, including role-based entitlements, workflow-based access requests and approvals, and provisioning/deprovisioning and revalidation of users as needed
- Secure access and storage of shared and privileged accounts
- Single sign-on with automated check-in and checkout of shared credentials
- End-to-end monitoring and reporting
- Out-of-the-box adapters to easily integrate the solution with operating systems, databases and third-party applications

Controlling the end-to-end lifecycle of privileged identities

IBM offers a comprehensive IAM solution that enables organizations to manage privileged access and reduce insider threats to enterprise security. IBM Security Privileged Identity Manager provides complete identity management and enterprise single sign-on capabilities for privileged users, delivering:

- Secure provisioning of privileged user accounts
- Automated password resets and management policies
- Activity logging for users of shared identities
- Automated processes that improve productivity, while strengthening security

Privileged identity management lifecycle



Security Privileged Identity Manager helps organizations strengthen their security postures by managing privileged access to systems and applications, across the enterprise and in the cloud. It enables organizations to avoid the high cost of privileged identity proliferation—by controlling shared access, tracking usage and automating password management.

Security Privileged Identity Manager helps organizations manage the entire lifecycle of privileged identities. Administrators are granted privileged access only to the systems and resources needed to perform their job roles. When they change jobs or leave the organization, their access rights are adjusted or revoked as necessary.

From the user's standpoint, the process is simple and seamless. When the user attempts to access a server or application, Security Privileged Identity Manager transparently checks out the required account credential on his or her behalf and automatically inserts the credentials to authenticate the user at the managed endpoint. The user will not know the logon credentials, and the password can be changed when the user's login session is terminated so that the user cannot use the login outside the secured login process.

By centralizing privileged ID management, automating check-in and checkout of credentials, and shielding passwords from users, Security Privileged Identity Manager improves IT governance and reduces risk. It also provides comprehensive tracking and reporting to enhance accountability and compliance by capturing when a privileged ID was used by whom and what the user did with that privileged ID.

Protecting resources with granular access control

Security Privileged Identity Manager helps thwart insider threats by securing and tracking the use of user credentials that have elevated access privileges. Some of its key features include:

- *Safe storage* of privileged account credentials
- A *shared identity service* that allows users to request access to a privileged account
- An automated and transparent *credential checkout and login process* from the user's Microsoft Windows desktop (including cloud-based virtual desktops)
- An extended *self-service user interface* that optionally enables users to perform manual checkouts and check-ins of credentials (an organization may choose to only allow automated checkouts and check-ins)
- *Timed auto check-in of account*, which is useful if a user fails to check in the account before expiration (lease times are configurable)
- A *password reset* that can be configured to execute at each check-in

System administrators, application owners, HR representatives, line-of-business managers and security personnel can all have elevated access within the Security Privileged Identity Manager solution. They can also manage access to non-privileged accounts using the same technology. This gives the organization a central place from which to manage identities, assign roles and configure policies that safeguard the entire infrastructure—including the cloud. Conversely, users can extend their existing IBM identity management or enterprise single sign-on deployments to add privileged identity control, thereby reducing IT cost and complexity.

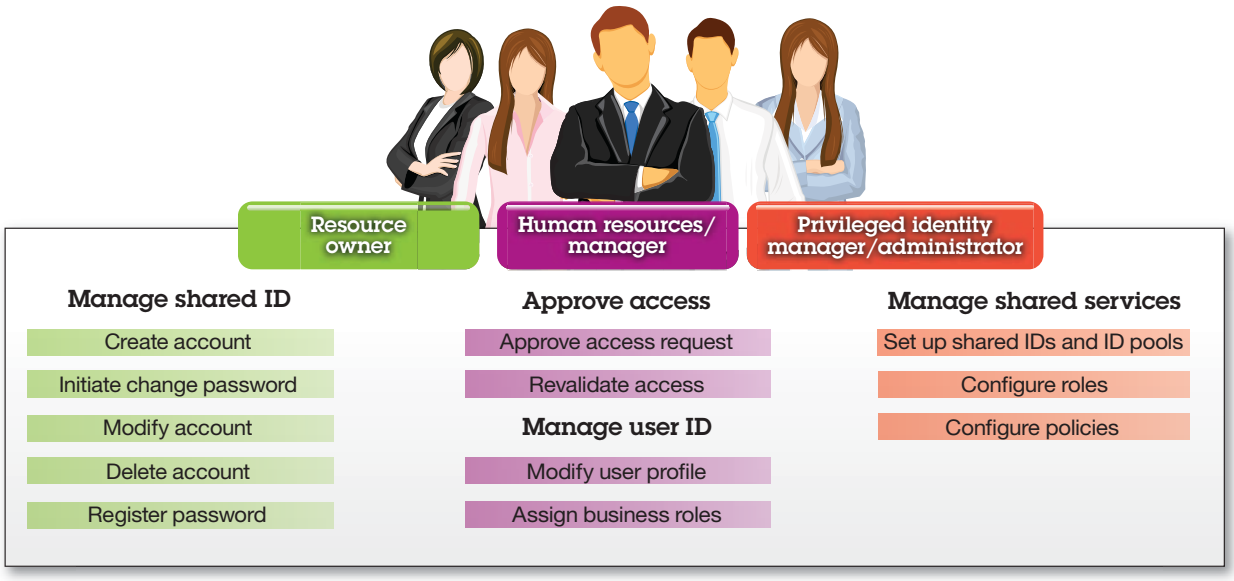
IBM use case: Reducing risks for a retail chain

With 1,200 store locations throughout the United States, a retail chain had expanded its IT staff to include 600 people spanning a variety of disciplines. Each IT staff member had an account on the company's 2,400+ servers, creating approximately 1,400,000 privileged accounts in the organization. In addition, a third-party audit found that a large number of store employee accounts were active even after those employees had been terminated. There were also incidents in which store employees extended fraudulent discounts to customers by using point-of-sale (POS) stations where a store manager had forgotten to log out.

IBM privileged identity management solutions gave the retail chain a centralized approach to rapidly provision, recertify and deprovision employees, and to reduce the costs and risks associated with having millions of privileged accounts. Now, the retailer can very narrowly limit access to sensitive payment and financial-related systems, databases and applications to only those employees with specific needs. This includes the ability to:

- **Define the accounts and levels of access for each employee's role**
- **Expedite the onboarding process (provisioning/deprovisioning) for store employees**
- **Secure and simplify in-store authentication to the POS systems**
- **Contain the escalating budget for IT staff**
- **Ensure compliance with industry standards**

Administrative-user flow architecture



Extending security intelligence with IBM

As a recognized worldwide leader in IAM services and solutions, IBM has the expertise to deliver effective privileged identity management. IBM understands how to help organizations confidently defend their business operations against insider threats, across traditional IT environments and into the cloud. IBM provides technology that is already used by organizations worldwide to reduce costs, improve security and help ensure compliance with common industry and government regulations. IBM Security Privileged Identity Manager delivers the comprehensive solution that IT organizations need to securely track and audit activities of privileged users for effective governance—and to reduce the risks of costly security breaches.

IBM operates the world's broadest security research, development and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the IBM X-FORCE® research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.

For more information

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

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

[1] CSO Magazine, "Most Fraud is an Inside Job, Says Survey." November 9, 2011. http://www.csoonline.com/article/693649/most-fraud-is-an-inside-job-says-survey

© Copyright IBM Corporation 2012

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

IBM, the IBM logo, ibm.com, 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

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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 client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

WGW03016-USEN-00