Tackle insider threats with IBM Security Privileged Identity Manager

Centrally manage and audit privileged user identities throughout the user lifecycle

Highlights

- Help reduce risk by simplifying and automating the administration of privileged identities
- Control check-in and check-out of shared IDs through a credential vault, effectively hiding passwords from the end user
- Reduce the total number of privileged IDs needed, enhancing security and boosting efficiency
- Facilitate compliance and audit support with optional capabilities for session recording, archive and replay
- Control and monitor the activities of privileged users without the need to deploy agents on their desktops
- Help reduce costs and speed time to value with a scalable, highly available virtual appliance and out-of-the-box reporting

Insider threats represent an alarming percentage of data breaches today—60 percent according to IBM security research.[1] The users you trust most with your sensitive information, customer data, business-critical applications and network assets—the resources that are the "crown jewels" of your business—are the people who have the potential to do the most damage to your organization, whether by accident or on purpose. In either case, a data breach perpetrated by an insider can wreak havoc on your operations and can cost you dearly, both financially and in terms of reputation.

Employees, contractors, business partners, outsourcing providers and other users are necessarily entrusted with shared and privileged access in order to do their jobs—and some are more privileged than others. But how do you ensure that your "super-users" are not abusing their privileges, leaking their credentials or harming the business, either unwittingly or maliciously? How do you ensure that the principles of least privilege are continuously enforced? How do you eliminate the anonymity of shared access? And how do you effectively control and monitor access across multiple networks and locations?

Tackling the challenges of shared and privileged access

Enforcing security by limiting access to sensitive assets, enforcing access policies and keeping detailed audit records is critical. But today's organizations are now called upon to monitor and record privileged user activity, and tightly manage shared passwords and login credentials to prevent abuse or compromise. They have to identify anomalous behavior and alert security administrators while there is still time to respond and potentially mitigate a malicious attack or remediate an access-related vulnerability.

IBM® Security Privileged Identity Manager is an identity and access management solution designed specifically to tackle the challenges associated with managing shared and privileged access in complex environments—from initial provisioning, recertifying and deprovisioning of secure credentials to the ongoing control and tracking of privileged user activity. IBM Security Privileged Identity Manager provides single sign-on capabilities for privileged users and enables authorized check-in and check-out of shared IDs from a credential vault, effectively hiding current passwords from the end user. It also reduces the total number of privileged IDs needed, improving overall security and efficiency.

The solution simplifies and automates privileged identity and password management activities across a broad array of targets, helping to eliminate the time, cost and human error associated with manual methods. And it helps organizations enforce strong privileged access policies and facilitates compliance with industry regulations such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, North American Electric Reliability Corporation (NERC) standards, the Federal Information Security Management Act (FISMA) and National Institute for Standards and Technology (NIST) Special Publication 800-53.

By providing comprehensive tools for centrally controlling and auditing the activities of privileged users throughout the user lifecycle, IBM Security Privileged Identity Manager helps prevent insider threats and identity-related fraud to protect data and systems against inappropriate access. As a scalable and highly available virtual appliance with an intuitive user interface and out-of-the-box reporting, the solution also helps organizations reduce administrative overhead and speed time to value.

Agent-less controls for shared credentials

A critical feature of IBM Security Privileged Identity Manager is the Privileged Session Gateway, which allows authorized users to use a web-browser interface to seamlessly check out and use privileged credentials to securely log in to a target application. This feature does not require installation of any agent software on the end user's desktop, providing organizations with the option for agent-less controls in addition to the solution's agent-based framework.

The Privileged Session Gateway feature can also be used with the optional Privileged Session Recorder tool, which encourages appropriate behavior by privileged users and enables organizations to demonstrate compliant access to those protected resources.

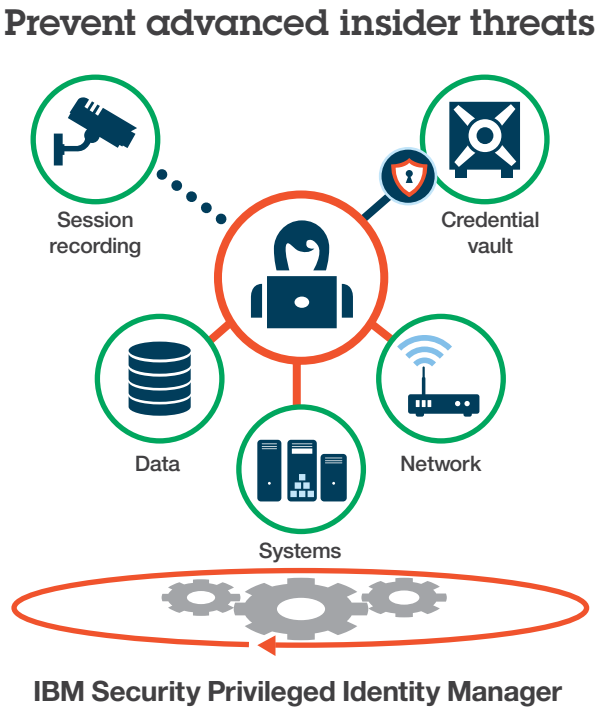
Comprehensive session recording

Privileged Session Recorder is an optional feature that enables full-session visual recordings of privileged user activities, as well as on-demand search and replay capabilities. With Privileged Session Recorder, each privileged user's session activity—including typed characters and mouse clicks—is recorded and stored for future access. Privileged Session Recorder provides clear audit visibility into the activities of privileged users and facilitates forensic research in the event of a security incident or for troubleshooting purposes.

Mitigating the insider threat

IBM Security Privileged Identity Manager helps mitigate sophisticated insider threats by providing a single solution for securing, automating and tracking the use of privileged access credentials across systems, applications and platforms. The solution delivers privileged user entitlement provisioning, strong password management policies and support for all IBM Security Identity Manager adapter endpoints.

The solution also provides control and visibility into privileged users' activities in the cloud environment, such as within IBM SoftLayer® cloud services. With IBM Security Privileged Identity Manager, SoftLayer cloud services customers can allow their system administrators to securely share SoftLayer portal administration credentials for customer service.



IBM Security Privileged Identity Manager provides a single solution for securing, automating and tracking the use of privileged access credentials across systems, applications and databases.

A holistic approach to security

IBM Security Privileged Identity Manager is an integral part of the holistic IBM approach to security—one that integrates seamlessly with complementary IBM Security products such as IBM QRadar® SIEM, IBM Security Identity Governance and Intelligence and IBM Security Guardium®, expanding the depth and scope of insider threat protection.

Critical to protecting against insider threats, IBM Security Identity Governance and Intelligence checks for segregation of duties violations and runs access certification campaigns to ensure validity of privileged access rights. QRadar SIEM provides comprehensive security information and event management (SIEM) capabilities, consolidating log events and network flow data from thousands of devices, endpoints and applications, and providing alerts on abnormal behavior. Guardium provides a full range of capabilities, including discovery and classification of sensitive data, vulnerability assessment, data and file activity monitoring, and comprehensive features to protect sensitive data, including masking, blocking, encryption, alerts and quarantine. These supplemental capabilities can help organizations better adhere to security regulations, protect sensitive assets and enhance their overall security posture.

Why IBM?

IBM Security solutions for identity and access management are trusted by organizations worldwide to safeguard, automate and track the use of privileged identities; improve identity governance; control how privileged IDs are shared to avoid the proliferation of these IDs and reduce associated costs; and strengthen 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 leverage 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 the IBM Security Privileged Identity Manager, please contact your IBM representative or IBM Business Partner, or visit the following website: **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
December 2016

[1] "2016 X-Force Threat Intelligence Report," *IBM X-Force Research*, February 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03114USEN&attachment=WGL03114USEN.PDF

Please Recycle

WGS03096-USEN-00