



# Privileged Identity Management

*An Executive Overview*

## Contents

What You Need to Know . . . . .	3
Privileged Identities Explained . . . . .	3
Risks of Unmanaged Privileged Identities . . . . .	4
How Privileged Access Spreads. . . . .	5
Business Drivers . . . . .	5
Mitigate Auditor Findings and Compliance Costs . . . . .	5
Control Insider Threats . . . . .	6
Mitigate Hackers and Malware . . . . .	7
Improve IT Staff Efficiency . . . . .	8
Implementation Challenges . . . . .	8
Best Practices . . . . .	9
Different Approaches Yield Different Results . . . . .	10
Ad-Hoc Methods . . . . .	10
Automated Management Processes . . . . .	10
Bottom Line . . . . .	12

## What You Need to Know

Each time you login to your organization's network you're required to enter a password to help keep the network secure from outsiders. Most networks also require you to follow basic rules when choosing your password to ensure that it cannot be easily compromised, for example:

- Your password may need to be of a minimum length,
- It may need to contain numbers or special characters,
- It may need to be different from other passwords that have you've chosen in the past, and
- It may need to be changed with some regularity.

Your organization's **Identity Access Management (IAM)** system enforces these rules for password security and determines what information and services you can access with your login. Because you login each time by entering your personal credentials, the automated records (or logs) that are created as you access information and services can make you accountable for your actions.

### *Privileged Identities Explained*

Individual user credentials aren't the only type of logins present on your network. The IT personnel who maintain servers, network components, and software use special passwords with elevated permissions needed to install new hardware and software, configure services, and service the IT infrastructure.

Called **privileged identities**, these logins allow unrestricted access to view and change data, alter configuration settings, and run programs. Typically associated with hardware and software assets (and not with any one user), privileged identities grant "super-user" access to virtually every resource on your network including:

- The operating systems that run all computer platforms,
- The directory services that control access to your network,
- Line-of-business applications, databases, and middleware,
- Network and security appliances,
- Backup and other service software and appliances,
- The hypervisors that manage the virtual machines (VMs) on your network.

*Privileged identities allow unrestricted access to view and change data, alter configuration settings, and run programs.*







Privileged accounts aren't used only by individuals. **Business applications** and **computer services** must also store and use privileged credentials to authenticate with databases, middleware, and other applications when requesting sensitive information and computing resources.

### Risks of Unmanaged Privileged Identities

Unlike end-users' personal login credentials, **privileged credentials are not systematically managed in most organizations.** This means that in all likelihood:

- Your organization has no comprehensive, up-to-date list of all the privileged logins that exist on your network;
- You have no verifiable record of which privileged login credentials are known to different individuals;
- You have no proof of who has used these privileged logins to gain access to any of your IT resources, when, and for what purpose;
- There is no way to verify that each of your privileged account passwords are cryptographically strong, are sufficiently unique, and are changed often enough to be secure;
- You have no complete list of privileged account passwords stored within your applications, and no way to know which in-house and vendor personnel have knowledge of these credentials that might be used to access sensitive information.

A summary of privileged identities present in a typical enterprise network, and the anonymous actions that can be taken by personnel with knowledge of these logins, are shown in **Figure 1 below.**

What Roles? ➡	What Assets? ➡	What Accounts? ➡	What Anonymous Actions?
<ul style="list-style-type: none"> <li>• System Administrators</li> <li>• Contractors</li> <li>• Integrators</li> <li>• Security Administrators</li> <li>• IT Managers</li> </ul>	Windows, Linux, UNIX, and Mainframe Computers 	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Root</li> <li>• Super User</li> <li>• Service</li> </ul>	<ul style="list-style-type: none"> <li>• Read, copy and alter data</li> <li>• Change security settings</li> <li>• Create and delete accounts</li> <li>• Enable and remove file shares</li> <li>• Run programs</li> </ul>
<ul style="list-style-type: none"> <li>• Security Administrators</li> <li>• IT Managers</li> </ul>	Directories 	<ul style="list-style-type: none"> <li>• Admin</li> <li>• Root</li> <li>• Administrator</li> </ul>	<ul style="list-style-type: none"> <li>• Read, copy, and alter user data</li> <li>• Add and delete users</li> <li>• Change user privileges</li> <li>• Enable remote access</li> </ul>
<ul style="list-style-type: none"> <li>• App Administrators</li> <li>• App Developers</li> <li>• Webmasters</li> <li>• Contract Developers</li> </ul>	Application Tiers 	<ul style="list-style-type: none"> <li>• Service</li> <li>• Config Files</li> <li>• ASP.Net</li> <li>• Run As</li> <li>• DB Connection</li> </ul>	<ul style="list-style-type: none"> <li>• Modify back-end applications</li> <li>• Alter public-facing websites</li> <li>• Read and change DB records</li> <li>• Access transaction data</li> </ul>
<ul style="list-style-type: none"> <li>• DB Administrators</li> <li>• App Developers</li> <li>• App Administrators</li> <li>• Contract Developers</li> <li>• Integrators</li> </ul>	Databases 	<ul style="list-style-type: none"> <li>• SA</li> <li>• Root</li> <li>• SYS</li> <li>• SYSDBA</li> </ul>	<ul style="list-style-type: none"> <li>• Read and change DB records</li> <li>• Access transaction data</li> <li>• Alter DB configuration and schema</li> <li>• Add and modify stored procedures</li> </ul>
<ul style="list-style-type: none"> <li>• Network Administrators</li> <li>• Security Administrators</li> </ul>	Network and Security Appliances 	<ul style="list-style-type: none"> <li>• Root</li> <li>• Enable</li> <li>• Admin</li> </ul>	<ul style="list-style-type: none"> <li>• Alter configuration settings</li> <li>• Change security and QoS policies</li> <li>• Grant and deny network access</li> <li>• Access data feeds</li> <li>• Enable and disable monitoring</li> </ul>
<ul style="list-style-type: none"> <li>• System Administrators</li> <li>• Backup Operators</li> <li>• Network Administrators</li> <li>• Contractors</li> </ul>	Backup and Service Infrastructure 	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Root</li> <li>• Super User</li> <li>• Service</li> </ul>	<ul style="list-style-type: none"> <li>• Browse and save archives</li> <li>• Access transaction data</li> <li>• Delete saved files</li> <li>• Change configuration settings</li> </ul>

**Figure 1 – Anonymous Actions Possible Using Unmanaged Privileged Identities**

## How Privileged Access Spreads

For the sake of convenience, IT personnel frequently configure common privileged account logins that are shared among numerous hardware and software resources and seldom change the passwords. As a result, privileged access can quickly spread over time as:

- New hardware and application rollouts take place, deploying more and more common privileged passwords that are known to many individuals;
- Changes in corporate structure such as mergers, IT outsourcing, and reorganizations occur, requiring changes in job roles and the disclosure of password secrets to more staff personnel;
- Workers with knowledge of privileged account passwords leave the organization and take password secrets with them;
- Unauthorized individuals and malware exploit cryptographically weak, reused, and infrequently changed privileged account passwords to extract login credentials without the organization's knowledge.

## Business Drivers

The motivation to implement privileged identity management processes often starts with an immediate need to address negative audit findings, or with an executive mandate to improve an organization's GRC (governance, risk management and compliance) posture. Additional business drivers can include the desire to lower recurring costs and uncertainty related to audit preparations, a desire to mitigate risks from internal and external threats, and a desire to improve IT staff efficiency as discussed in the following sections.

### Mitigate Auditor Findings and Compliance Costs

Today's regulatory mandates can introduce significant costs as organizations undergo recurring efforts to document compliance. Failure to maintain compliance with current standards can result in direct penalties, negative press exposure, and significant costs as personnel work to address the negative findings. Fortunately, prevailing regulatory standards (including SOX, PCI-DSS, HIPAA, and others) share largely common requirements when it comes to securing privileged identities.

To address the major regulatory frameworks, at a minimum privileged identity management processes should:

- Document the presence of all privileged account logins – including administrative logins and the credentials used by applications and services – on all hardware platforms.
- Fully document which individuals are authorized to access each IT resource and account.
- Provide historical logs to document a policy of “least privilege” by showing who has actually requested access to each IT resource, when and for what purpose.

*The motivation to improve privileged identity management processes often starts with an immediate need to address negative audit findings, or with an executive mandate to improve the organization's GRC (governance, risk management and compliance) posture.*

- Institute an auditable process to change privileged passwords immediately after each access so that the logins cannot be reused without a subsequent record.
- Establish a means to alert management to any unusual activities.
- Provide a way to document that every hardware and software asset is covered by the organization's access policies.

As discussed in the following sections, software solutions are available to automate these steps, thereby significantly reducing IT staff overhead.

### Control Insider Threats

According to a 2010 report,<sup>1</sup> 48% of data breaches are caused by insiders. And while many organizations employ measures such as physical locks and ID keycards to control physical access, most lack the processes needed to control the privileged access that allows individuals to view and change data records or alter configuration settings at any time over the network.

Recent events demonstrate how failure to safeguard privileged access can result in the loss of sensitive data and failures in business-critical services:

- A senior IT administrator at a large financial services company was accused of stealing and selling sensitive bank account and credit card information of 2.3 million customers.
- A pharmaceutical supplier discovered the presence of a logic bomb inserted by an administrator before company-wide layoffs; the malicious code was designed to destroy the company's clinical trial data.
- A large US city was locked out of its network by an administrator who was arrested following an altercation on the job.

Headlines from recent news stories are shown in **Figure 2 below**. In addition to negative press reports and damage to reputation, in each case the victim organization incurred significant costs to remediate the breach, suffered penalties and fines, or both.



**Figure 2 – Victim Organizations in the Headlines**

<sup>1</sup> "2010 Data Breach Investigations Report," Verizon RISK Team in cooperation with the United States Secret Service.

To mitigate the risks of insider threats, organizations work to create a climate of accountability by instituting checks and balances in their IT management processes. A critical element is the control of administrative access to databases, servers, supporting applications, and other components that host sensitive data. Privileged identity management processes can enable organizations to enforce principles of “least privilege,” documenting that individuals utilize only the level of permissions needed to do their job while minimizing the likelihood of damaging data breaches and unintended service outages.

### **Mitigate Hackers and Malware**

Today more than 90% of records stolen by hackers are obtained through breaches in web applications.<sup>2</sup> For this reason securing the privileged credentials in internet-facing applications and ancillary tiers (including databases, middleware, and so on) is a critical step to improve an organization’s GRC posture.

To better secure an organization against hackers and malware, an effective privileged identity management process should:

- Discover and document the presence of privileged account logins in web application tiers, packaged software programs, line-of-business applications, custom programs and other applications – whether the credentials are encrypted, stored in plain text files, or compiled into the applications themselves;
- Track the interdependencies of all application tiers to ensure that each password change is synchronized among interdependent applications to avoid service disruptions and lockouts;
- Secure each embedded application password by ensuring that it is cryptographically complex, unique from other application passwords to the extent possible, and frequently changed.

A 2009 US Congressional report<sup>3</sup> outlining organized hacker attacks (otherwise known as Advanced Persistent Threats, or APTs) documents how attackers can leverage “highly privileged administrative accounts” to penetrate victim organization networks once gaining access through a single compromised computer. Because a sound privileged identity management process can secure both application passwords and the privileged logins used by personnel, it can help organizations mitigate the risks of hackers and malware by:

- Decreasing the likelihood of successful, external attacks on internet-facing applications;
- Eliminating common and easily-guessed privileged account passwords that allow hackers and malware to easily exploit additional systems should a single computer be compromised;
- Eliminating the possibility of unauthorized personnel (including former contract developers, software vendors, and others) retaining application logins that could allow them to view and change data or alter configuration settings after their roles have changed.

*Because more than 90% of data records are stolen through breaches in web applications, securing the privileged credentials in web-facing applications is a critical step to improve your GRC posture.*

<sup>2</sup> Ibid.

<sup>3</sup> “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” The US-China Economic and Security Review Commission, October 2009

### *Improve IT Staff Efficiency*

In addition to improving an organization's GRC posture, effective privileged identity management processes can improve staff efficiency by introducing the means to:

- Follow repeatable processes that reduce the time needed to maintain up-to-date lists of privileged accounts present on software and hardware resources;
- Reduce the time and uncertainty of changing privileged account passwords through use of up-to-date documentation of the accounts;
- Eliminate the time and uncertainty of obtaining approvals and retrieving passwords when needed to access systems for routine maintenance and emergency repairs;
- Automate the tasks to document the presence of privileged accounts and their access history, as required by regulatory standards;
- Support root-cause analysis to more quickly determine the reasons for undesired changes; giving staff the tools to know who requested privileged access to IT assets in question, when, and for what purpose;
- Eliminate staff time taken to remediate negative audit findings that would otherwise occur.

## **Implementation Challenges**

In most organizations, technological and human barriers make it necessary to carefully plan the implementation of privileged identity management processes, and to gain executive management support early-on in the project. Technological roadblocks can include:

- Frequently-changing networks with heterogeneous hardware and software platforms;
- Large numbers of frequently changing target systems that can be separated by slow, unreliable, or expensive WAN links;
- Complex organizational structures with overlapping and frequently-changing lines of delegation and control;
- Combinations of new, legacy, and in-house applications that may store privileged credentials in a variety of ways – ranging from secure, encrypted formats to more vulnerable plain-text files and direct compilation into the applications themselves.

Beyond the technological challenges, the introduction of privileged identity management processes also requires fundamental changes in how sensitive credentials are disclosed and attributed to those who use them. Regardless of whether the process lowers staff workloads, individuals who once enjoyed unlimited, anonymous access will likely resist being held accountable. For this reason the project is likely to succeed only with the active sponsorship of top management.

## Best Practices

Effective privileged identity management is a continuous cycle as represented in **Figure 3 below**.



**Figure 3 – Privileged Identity Management Cycle**

The process can be represented in four phases, abbreviated as I.D.E.A.:

- Identify and document all critical IT assets, their privileged accounts and interdependencies wherever present on any hardware or software platform;
- Delegate access to credentials so that only appropriate personnel, using least privilege required, with documented purpose, can login to IT assets in a timely manner at designated times;
- Enforce rules for password complexity, diversity and change frequency, synchronizing changes across all dependencies to prevent service disruptions;
- Audit, alert and report so that the requester, purpose, and duration of each privileged access request is documented and management is made aware of unusual events.

### *Defining Project Goals*

From the beginning each implementation should start with a discussion among all stakeholders including the CSO, CIO, IT administrators, and others involved in the management of sensitive accounts. The key stakeholders should be those that will suffer the most damage should the process take too long to implement, unnecessarily add to staff workloads, or provide insufficient coverage.

Define overall project goals and then decide who on the team is best suited to determine whether the proposed implementation is really a fit. At the very least, the outputs of the process should include:

- A detailed, written analysis of your organization's business goals;
- Explicit documentation of your needs with respect to systems, applications, and lines of control;
- A clear statement of work that details the time and cost required to manage the unsecured privileged accounts present in your target systems and applications, once a solution is chosen.

### *Preparing Your Environment*

Before privileged identity management processes are put in place, it is important to correct any improperly conceived account names and assignments that may have been configured by previous generations of IT staff. For example, you'll likely want to ensure that every database service account is assigned a different domain login so that you can release credentials with limited scope rather than disclosing any logins that have broad, elevated permission to make changes across your enterprise. The same holds true with all other types of privileged accounts; better governance requires you to organize these credentials to limit the scope of access.

By taking this step you can avoid the mistake of simply automating poor prior practices. IT security administration tools – including those from Lieberman Software – can greatly reduce the time needed to complete these preparations.

## **Different Approaches Yield Different Results**

### *Ad-Hoc Methods*

It can take a great deal of staff time and process discipline to identify and track all privileged accounts and interdependencies on a large network using manual and ad-hoc methods. To enumerate privileged identities without the use of dedicated software, an organization's IT staff typically starts by exporting lists of IT assets from existing directory services. Connections are then established to each system through a combination of scripts that document the presence of system accounts, and by manual inspection for the presence of target applications and services.

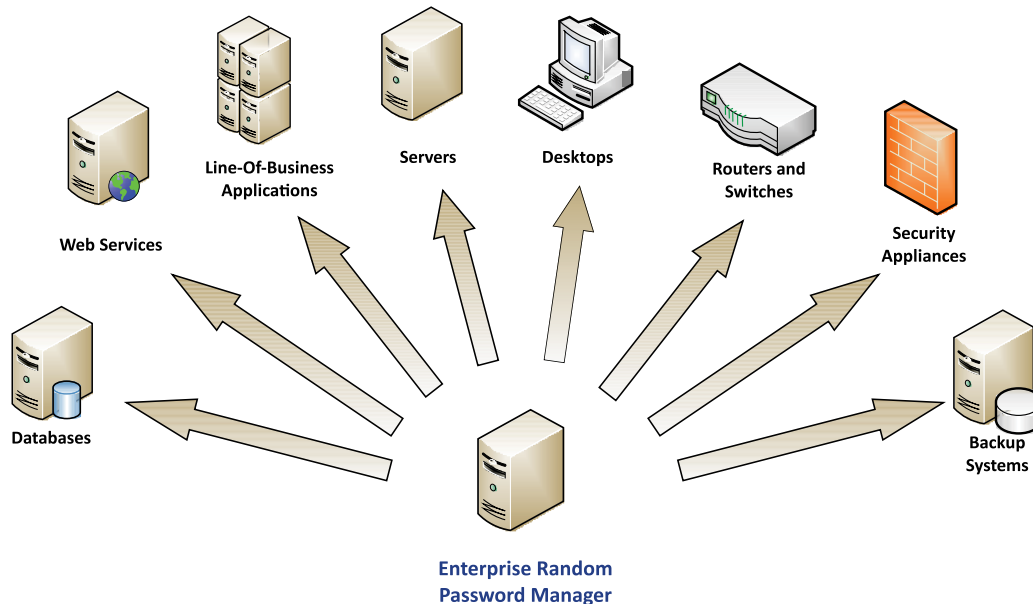
Because this process is time-consuming and varies widely from system to system, it carries the risk that personnel will fail to consistently complete it. Further, maintaining an up-to-date catalog of identities and interdependencies requires that the process be repeated over time and with each significant change in infrastructure.

Lack of automation can create a significant burden for IT staff. As a security analyst at a large financial institution said of the manual tasks, "It's like painting the Golden Gate Bridge – starting at one end, working your way to the other end, and then starting all over. Essentially by the time you were done changing service account passwords you would have to start all over again."

### *Automated Management Processes*

Privileged identity management software can automate the task to catalog an organization's privileged accounts and interdependencies and help to assure that the results are complete and up-to-date. The best of these solutions can draw from numerous sources to create exhaustive lists of privileged identities present in the environment.

As represented in **Figure 4, Enterprise Random Password Manager (ERPM)** from Lieberman Software auto-discovers and catalogs privileged accounts present on a wide range of server and desktop operating systems, network and backup appliances, databases, Web services, line-of-business applications, and other IT resources.



**Figure 4 – Enterprise Random Password Manager (ERPM) from Lieberman Software**

ERPM detects and reports every location where privileged accounts are used – including local and domain accounts, configured services, scheduled tasks, applications including COM+ and DCOM, IIS websites, databases such as Oracle, SQL Server, and so on – and then rapidly propagates password changes everywhere that each account is referenced in order to prevent account lockouts and service failures that can otherwise occur when manual processes deploy obsolete credentials.

ERPM identifies, safeguards and manages the privileged identities found throughout the datacenter, including:

- **Super-user login accounts** utilized by individuals to change configuration settings, run programs and perform other administrative duties.
- **Service accounts** that require privileged login IDs and passwords to run.
- **Application-to-application passwords**, the credentials used by web services, line-of-business applications, custom software, and virtually every other type of application to connect to databases, middleware, and other application tiers.

ERPM secures its passwords in an encrypted database that can be accessed from any web-enabled device. Users check out privileged account passwords through an automated process that takes advantage of an organization's existing identity access management framework to allow expedited, delegated access. Passwords are automatically re-randomized after check-in, and limited to restricted recovery periods, forced check-ins, periodic verifications, and web session timeouts. Phonetic spelling options are provided.

## Bottom Line

As IT auditors become more aware of the threats posed by unmanaged privileged identities your organization could face increasing pressures to bring these powerful logins under control. Hackers have also taken notice, increasing the frequency of attacks that exploit shared, elevated credentials to gain control of victim organizations' networks.

Fortunately, privileged identity management software can help you continuously secure privileged credentials throughout your network and provide an authoritative audit trail of their access. A successful implementation can also save IT staff time by providing login credentials instantly and on-demand, reducing the need for manual processes to discover, change, and document the accounts.

## Next Steps

Organizations that desire more insight into potential risks of the unsecured privileged accounts in their IT environments can contact Lieberman Software for an ERPM software trial. ERPM documents potential risks present in the infrastructure and enumerates privileged accounts by hardware platform, account and service type. It then continuously secures privileged accounts everywhere on your network and provides an audit trail of each access request. ERPM trial software is available at no cost to qualified organizations. For more information, email [ERPM@Liebsoft.com](mailto:ERPM@Liebsoft.com).



**[www.liebsoft.com](http://www.liebsoft.com) | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152  
1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067  
© 2010 Lieberman Software Corporation. Trademarks are the property of their respective owners.**