

Who Holds the Keys to Your IT Kingdom?

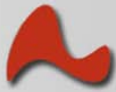
Four Key Steps to Securing Privileged Identities



Executive Summary

Because privileged identities hold elevated permissions to access data, run programs and change the configuration settings on virtually every hardware and software component of IT, control over their use is essential to maintain information security and operational efficiency. Regardless of past audit successes, organizations that fail to adequately control the use of privileged identities have experienced data loss, downtime, and damage to reputation.

This guide examines four key steps necessary to secure an organization's privileged identities. It describes basic, manual and ad-hoc processes that can improve control over privileged access along with automated alternatives to further reduce the risks of data breaches and operational disruptions while improving staff efficiency and management oversight.



Contents

Executive Summary.....	1
Introduction	3
About Privileged Identities	3
How Access to Privileged Identities Spreads	3
Privileged Identities – The Risks.....	3
Privileged Identities and Compliance	5
Privileged Identities and IT Service Management	7
Taking Control.....	8
Step 1 – Identify	8
Manual and Ad-Hoc Processes to Identify Privileged Accounts.....	9
Automated Alternatives to Identify Accounts and Interdependencies.....	9
Step 2 – Delegate	10
Manual and Ad-Hoc Processes To Delegate and Control Access	10
Automated Alternatives for Delegation and Secure Access.....	11
Step 3 – Enforce	12
Manual and Ad-Hoc Processes to Enforce Password Rules.....	12
Automated Alternatives to Enforce and Propagate Password Rules	13
Step 4 – Audit.....	14
Manual and Ad-Hoc Auditing Processes.....	14
Automated Alternatives for Auditing and Alerting.....	15
Next Steps	16
Summary	16
About Lieberman Software.....	16

Introduction

About Privileged Identities

Privileged identities are accounts that hold elevated permission to access files, run programs, and change configuration settings. Privileged identities exist virtually everywhere in IT; they are found on server and desktop operating systems, on network devices such as routers, switches, and security appliances, and in programs and services including databases, line-of-business applications, Web services, backup software, scheduled tasks, and others.

The Identity Access Management (IAM) technologies that are present in virtually all IT environments are designed to provision and de-provision users, manage normal user login activity, and may grant single sign-on to multiple systems and applications. However, in general these technologies don't detect or secure privileged identities.

How Access to Privileged Identities Spreads

Absent sufficient controls, access to an organization's privileged accounts spreads over time in both planned and unintended ways. This happens as:

- Companies fail to change the pre-configured logins and service accounts (whether documented or undocumented) that are introduced as they deploy new hardware such as servers, networking appliances, backup systems and monitoring appliances.
- New applications are installed that contain both documented login and service accounts and undocumented backdoors.
- Companies delegate administrative duties across overlapping functional teams, change the roles of administrative personnel, and contract these duties to outside personnel.
- Organizations fail to revoke all privileged accounts accessed by an employee after his job role changes or his employment ends.
- Password security is breached by social engineering, dictionary attacks, and other means.

Because privileged identities are found virtually everywhere in the infrastructure and their access tends to expand over time, they can pose significant risks of unwanted data access and disruptions in business-critical services.

Privileged Identities – The Risks

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



- A US financial institution discovered that its domain login credentials had been published on the Internet by a fired IT administrator.¹
- A large US city was locked out of its network by an administrator who was arrested following an altercation on the job.²
- A pharmaceutical supplier discovered the presence of a logic bomb inserted by a disgruntled administrator with unmonitored access; the malicious code was designed to wipe out the company's clinical trial data.³
- A credit reporting agency exposed more than eight million consumers' personal data when its database administrator sold the data for personal gain^{4,5}.
- A PCI DSS-certified credit card processor suffered a data breach that it said had the potential to expose more than 100 million credit card accounts.^{6,7}



Figure 1 – Organizations That Become Victims of Security Breaches in the Headlines

Beyond direct financial losses and negative media exposure expressed in Figure 1 above, the lack of adequate policies and practices to manage privileged accounts can make an organization unable to:

- Realistically quantify and address its security risks by determining where all potential privileged account vulnerabilities reside
- Protect the organization's assets by verifying that sensitive data is accessible only by those who are intended to see it
- Safeguard operational stability and security by providing an audit trail of individuals who are granted access to sensitive data or to make changes to business-critical IT processes

¹ Immediately after the incident the organization purchased Lieberman Software products to secure its privileged identities.

² Paul Venezia, "Sorting Facts from Fiction in the Terry Childs Case," PC World, 30 July 2008.

³ Frank Washkuch Jr., "Former New Jersey systems administrator gets 30 months in prison for 'logic bomb'," SC Magazine, 9 January 2008

⁴ Asa Aarons, "Company reports huge breach in personal data," New York Daily News, 7 September 2007

⁵ Jaikumar Vijayan, "Database admin steals 2.3M consumer records at Fidelity National subsidiary," Computerworld Security, 3 July 2007

⁶ Linda McGlasson, "Heartland Data Breach: Visa Questions Processor's PCI Compliance," Bank Info Security 24 March 2009

⁷ Stefanie Hoffman, "Heartland Data Breach Could Leave 100 Million Accounts Exposed" ChannelWeb, 21 January 2009

- Maintain staff efficiency by ensuring that IT personnel have the resources necessary to comply with corporate security policies
- Eliminate inefficient, incomplete manual processes that can waste time while failing to address significant vulnerabilities
- Control the potential for extended damage after a single security breach exposes privileged account credentials that are re-used across independent IT assets
- Eliminate the potential for undesired system changes and service disruptions when privileged accounts are used for tasks that don't require them

Neglecting to control privileged account access can also lead to compounded costs as greater numbers of IT auditors look for sound management practices and more compliance authorities penalize organizations that fail to effectively address the risks.

Privileged Identities and Compliance

Failure to effectively manage privileged account access has the potential to block compliance with a range of initiatives and may lead to higher, direct business costs. For example, organizations processing credit card payments that fail to comply with Payment Card Industry Data Security Standards (PCI DSS) pay increased commissions and fines.⁸

Standards such as PCI DSS set minimum requirements for discovery of privileged accounts on *all* hardware and software assets along with restrictions on user access, account separation, auditing, password strength and reuse. Examples of PCI DSS requirements⁹ that are addressed by privileged identity controls are listed in Table 1 below.

What You Can Do

If you're concerned about the risks of unsecured privileged accounts in your IT environment you can contact Lieberman Software for an Enterprise Random Password Manager (ERPM) software trial.

ERPM discovers privileged accounts present in your infrastructure and documents the risks by hardware platform, account and service type. ERPM 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.

⁸ Jaikumar Vijayan, "Visa Warns Merchants of Deadline for PCI Compliance," Computerworld, 20 August 2007

⁹ PCI Security Standards Council LLC, "PCI DSS Requirements and Security Assessment Procedures v1.2," October 2008



2.1	"Always change vendor-supplied passwords before installing a system on the network..."
6.3.6	"Removal of custom application accounts, user IDs, and passwords before applications become active..."
7.7.1	"Restriction of access rights to privileged user IDs to least privileges..."
7.2.1	"Coverage of all system components."
8.5.4	"Immediately revoke access for all terminated users."
8.5.5	"Remove/disable inactive user accounts at least every 90 days."
8.5.6	"Enable accounts used by vendors for remote maintenance only during the time periods needed."
8.5.8	"Do not use group, shared, or generic accounts or passwords."
8.5.9	"Change user passwords at least every 90 days."
10.2	"Implement automated audit trails for all system components..."

Table 1 – PCI DSS Requirements Addressed By Privileged Identity Management

It can be argued that the PCI DSS requirement that *all* IT components have access controls in place cannot be realistically met without the use of software that continuously auto-detects and auto-remediates privileged account credentials. Like the PCI DSS – certified payment processors who have endured highly-publicized security breaches impacting millions of customers, companies that fail to continuously detect and control all privileged accounts can face significant vulnerabilities regardless of past certification. As an engineer at one network appliance vendor put it,

"Our appliances monitor the core switches at the majority of the Fortune 500. Years after deployment, customers have told us that they haven't changed the default logins and privileged service account passwords on these devices. Many of those organizations – including supposedly PCI DSS compliant ones – either don't know how to find all of the privileged service accounts on the appliances or are unwilling to make changes for fear of causing service outages."

Requirements to secure privileged identities appear in regulations on publicly-traded companies, healthcare and insurance firms, power generation and distribution companies, and numerous others. For example, Table 2 below lists HIPAA regulatory requirements to secure electronic healthcare records that are addressed by privileged identity management.



45§164.308(1)(D)	Implement audit logs, access reports, and security incident tracking reports.
45§164.308(3)(i)	Prevent unauthorized members from obtaining access.
45§164.308(3)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
45§164.308(3)(C)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends.
45§164.308(5)(C)	Implement procedures for monitoring log-in attempts and reporting discrepancies.
45§164.308(5)(D)	Implement procedures for creating, changing, and safeguarding passwords.
45§164.312(a)(1)	Allow access only to those persons or software programs that have been granted access rights.
45§164.312(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.
45§164.312(2)(b)	Implement mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Table 2 – HIPAA Requirements Addressed By Privileged Identity Management

The failure of seemingly compliant organizations to discover and control all privileged identities appears to be raising alarm with more and more auditors serving a wider range of industries. As Philip Lieberman, president of Lieberman Software, notes,

"As late as 2007 we rarely heard about audit failures resulting from the lack of a privileged identity management strategy. Today a sizeable percentage of our new customers are enterprises that face expensive compliance failures and are looking to regain control of privileged identities, improve security, and pass future audits."

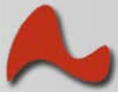
Privileged Identities and IT Service Management

Apart from compliance with Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, California Security Breach Information Acts, NASD 3010, SEC 17a-4, 21 CFR Part 11, DoD 5015.2 and a host of other regulations, organizations' failure to take control of privileged identities can impact the success of their IT service management processes. As one authority on ITIL, the most widely accepted approach to IT service management¹⁰ puts it,

"We must be aware of changes on all infrastructure that we are managing: servers, routers, network devices, databases, and so forth. Each detected change must either map to authorized work, or it must be flagged for investigation."¹¹

¹⁰ APM Group Ltd., "Official ITIL® Website"; <http://www.itil-officialsite.com/home/home.asp>; accessed 24 June 2004

¹¹ Kevin Behr, Gene Kim, and George Spafford, *The Visible Ops Handbook* (IT Process Institute, 2005) , p. 28



A common principle of IT service management is to control which personnel can make changes that have the potential to impact business-critical services, ensuring that changes are made only at designated times and only for documented purposes. In particular, the existence of super-user identities that allow unrestricted, undocumented access is viewed as an overreaching threat to successful IT service management:

"What is often overlooked is that if one person can single-handedly save the ship, that one person can probably single-handedly sink the ship, too." ¹²

As with other initiatives, failure to invest in sufficient safeguards to control privileged identity access can put IT service management processes at risk.

Taking Control

While the spread of uncontrolled privileged access threatens data security and operational efficiency, processes exist that can reliably help organizations regain control in a cost-effective manner. The processes can be described as four key steps that are abbreviated as *I.D.E.A.*:

- **Identify** and document all critical IT assets, their privileged accounts and interdependencies.
- **Delegate** access to credentials so that 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** and alert so that the requester, purpose, and duration of each privileged access request is documented and management is made aware of unusual events.

The following sections describe a number of alternatives to achieve these four steps.

Step 1 – Identify

The first step to take control of privileged identities is to identify where the account credentials reside on server and desktop operating systems, network appliances, software and service accounts, and elsewhere. A single server, for example, may have privileged identities present on domain and local logins, installed applications, scheduled tasks, services, IIS application pools, COM+, and DCOM objects. Without the assurance that *all* privileged identities are accounted for on every device, any initiative to take control of privileged access leaves significant gaps.

A second, critical aspect of this step is to thoroughly map the interdependencies among all privileged accounts on every device. Failure to take into account, for example, that a database

¹² *ibid.*

account is accessed by four dependent services on other computers means that changing database credentials alone will lock out the dependent services and create business disruption.

Because manually identifying substantially all privileged accounts and interdependencies requires a great deal of process discipline and a significant recurring effort, the use of automated software can improve the reliability of the process while substantially reducing the effort required.

Manual and Ad-Hoc Processes to Identify Privileged Accounts

To enumerate an organization's privileged identities without the use of dedicated software, IT staff typically start 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, to maintain an up-to-date catalog of identities and interdependencies requires that the process be repeated over time and with each significant change in infrastructure.

Automated Alternatives to Identify Accounts and Interdependencies

Privileged identity management software automates the task to catalog an organization's privileged accounts and interdependencies and helps 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 2 below, 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.

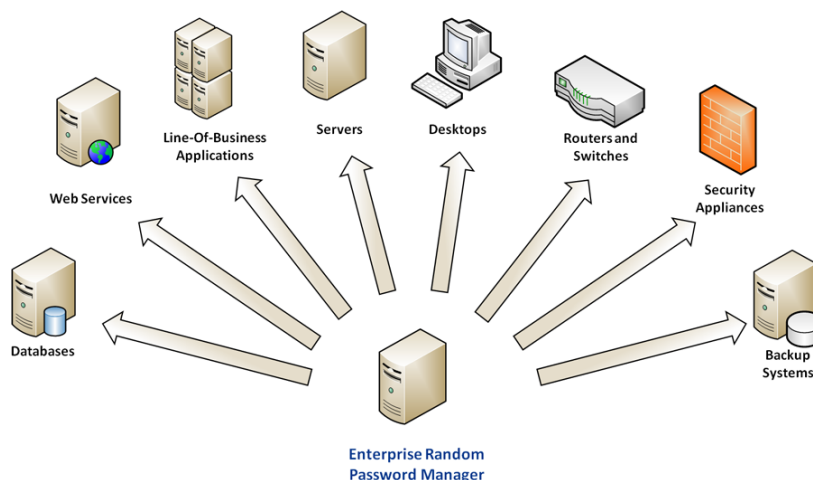


Figure 2 – ERPM Identifies a Wide Range of Privileged Accounts and Interdependencies



Figure 3 below shows how ERPm is configured to synchronize its discovery mechanism with Active Directory, one of many configurable discovery sources, to maintain its inventory lists.

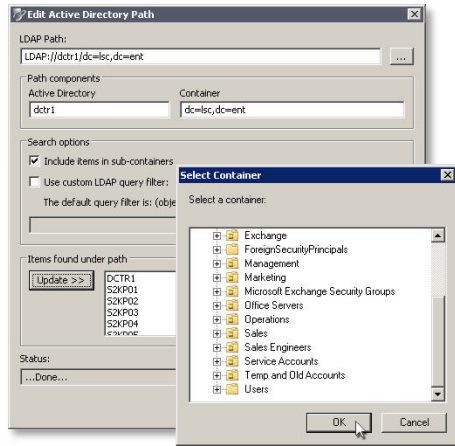


Figure 3 – Configuring Dynamic Discovery through Active Directory in ERPm

Among privileged identity management solutions, ERPm is distinguished by its ability to leverage a wide range of discovery sources – including the directory services of Microsoft, IBM, HP, Novell, Oracle, SAP, Sun, Siemens, Red Hat and other open source alternatives, domain browser lists, IP range scans, and others – and for its power to detect interdependent processes and auto-propagate the necessary changes, thereby preventing lockouts and service disruptions.

Step 2 – Delegate

A second key goal of privileged identity management is to grant access only to authenticated requestors, in a timely manner, over a secure communication channel for a predetermined length of time and a documented purpose, using the least privilege required.

Manual and ad-hoc methods to achieve this step face a number of security and accountability limitations, as will be examined in the next section.

Manual and Ad-Hoc Processes To Delegate and Control Access

The cornerstone of manual processes for granting privileged access is carefully-planned human and physical security. When manual processes are implemented the individuals who control password delegation should be thoroughly vetted and limited in number, and password credentials that are kept on spreadsheets and hard-copy lists must be safeguarded to make them inaccessible to all but authorized individuals. Regardless of the human and physical security measures that may be in place, manual processes introduce risks that can be difficult to mitigate:



- Because they lack automated auditing and control, they place a higher burden on an organization to thoroughly screen the individuals who control access.
- Manual processes make it more difficult to tie access to single individuals, since at a minimum a grantor and requestor both have access to passwords during each request.
- They increase the potential for service disruptions in distributed and 24-hour enterprises because they require at least one individual who controls the accounts to always have access to the credentials and a secure communication channel to each requestor.
- They make it more difficult to comply with service management initiatives because they rely on individual supervisors to document the reason for each access request and to communicate this data to those responsible for supervising the process.
- They can reduce overall security by relying on administrators to manually change the login credentials after a specified time following each request.

Automated Alternatives for Delegation and Secure Access

Automated privileged identity management software offers improved security, since it can:

- Promote greater accountability by delivering privileged credentials over a secure communication channel only to the authorized requestor, without exposing password secrets to any other individual.
- Provide 24-hour access to privileged credentials (including fire call access) anywhere in the world, authenticating through a configurable choice of directory and two-factor methods (Figure 4 below), regardless of the availability of supervisory personnel.

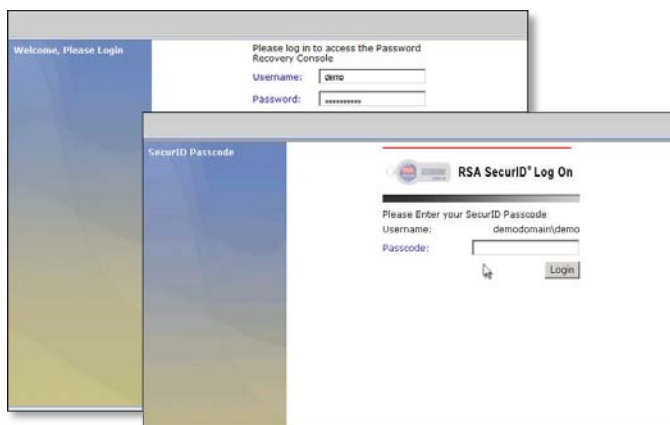


Figure 4 –Two-Factor Requestor Authentication in ERPM Using an RSA SecurID® Token

- Eliminate service disruptions and facilitate service management controls by providing a mechanism for requestors to document the purpose of each access, thereby giving



supervisory personnel a way to confirm that each access was necessary and used least required privilege.

- Eliminate misuse of credentials by changing the disclosed password automatically upon expiration of a pre-determined check-out time.

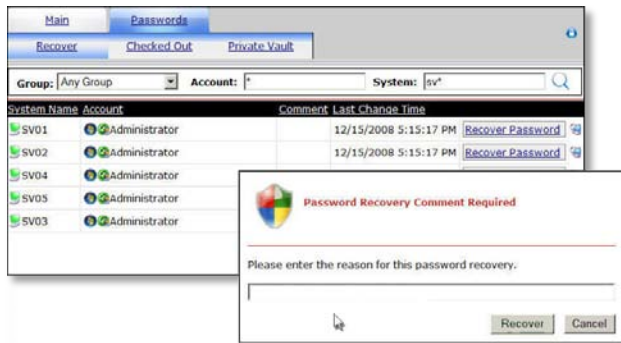


Figure 5 – Secure Web Interface for Password Recovery in ERPM

ERPM allows password self-recovery through an encrypted Web interface (Figure 5 above) that supports full auditing and reporting, and can be configured to require the requestor to enter a reason for each password checkout. This provides a mechanism for managers to verify that least required privileges were granted in each event.

Step 3 – Enforce

Reliably-enforced rules for password complexity, diversity (that is, avoiding unnecessary duplicate logins) and change frequency are critical to prevent the spread of uncontrolled access. As will be discussed below, manual processes to enforce password rules and update privileged account credentials face limitations that can impact both security and operational stability.

Manual and Ad-Hoc Processes to Enforce Password Rules

Organizations that rely on manual processes to enforce password strength, diversity and change frequency face a balancing act, since requirements that are too simple make systems vulnerable to automated exploits while complexity and change frequency policies that are overly stringent can make passwords impractical to remember and so induce employees to write down passwords and store them in other insecure ways¹³.

The re-use of login credentials across independent assets is also known to carry significant risk, as this practice exposes all assets with common passwords should one system be compromised. Therefore a common, ad-hoc practice that attempts to create more varied and robust

¹³ Ant Allan, "Blindly Increasing Password Strength Is Futile," Gartner 19 August 2008



passwords among systems in a group (say, servers in a single datacenter) is to use startup scripts that change passwords on each system based on combinations of variables such as computer ID and date. Because these scripts are typically accessed by several individuals during configuration, debugging and use, the effect is to share password secrets (and thus privileged access) among several employees. This makes it impossible to tie data access or a configuration change to any one person. Scripted methods may also lack appropriate logging features, may fail to consistently flag and handle error conditions, and can rely on serial processes that fail to reliably synchronize changes across interdependent assets.

Automated Alternatives to Enforce and Propagate Password Rules

Privileged identity management software makes complying with password strength, diversity and change rules less burdensome for administrators while making it easier for authorized requestors to access privileged accounts. These solutions improve the security of the process because they:

- Deploy diverse passwords of predetermined complexity on all target systems according to a schedule
- Can present unique, privileged credentials for one-time use over a secure interface
- Can change passwords immediately after each use

The straightforward interface in ERPM to configure password complexity and the frequency of changes is shown in Figure 6 below.

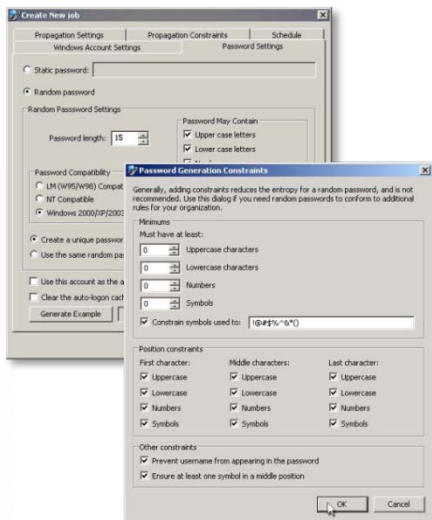


Figure 6 – Configuring Password Complexity Settings in ERPM

Just as importantly, the best of the automated solutions detect the presence of interdependent accounts and can reliably propagate password changes across them. This eliminates the potential for service disruptions that occur as dependent services are locked out after failing to



receive updated credentials. The most easily configured of these solutions offers a simple interface to set propagation rules, as with ERPM in Figure 7 below.

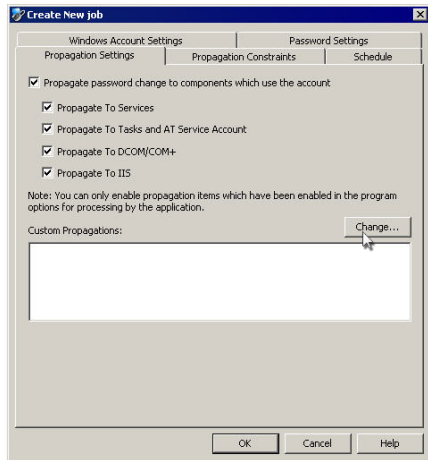


Figure 7 – Configuring Automated Propagation Settings in ERPM

ERPM is typically configured to re-randomize each password following a defined period after password checkout, thereby eliminating the opportunity for credentials to be shared or re-used for undocumented purposes. The result is improved auditing control, as will be discussed in the following section.

Step 4 – Audit

Beyond their value in assuring compliance with regulatory and industry requirements, the presence of reliable auditing and alerting processes can improve operational efficiency by reinforcing service management rules and setting guiding values among employees that lead to stronger adherence to management directives.

Because manual and ad-hoc privileged identity management processes make it difficult to ensure that each access is documented in a consistent way, they can lead to incomplete reporting and an audit trail that is of little use to enforce the organization's policies. Conversely, automated auditing features found in privileged identity management software can reliably log and report each access request, report access activity and trends in ways that can help pinpoint infrastructure and organizational problem areas, and alert supervisory personnel to unusual events such as fire call access and process faults.

Manual and Ad-Hoc Auditing Processes

As noted above, manual processes rely on supervisory personnel to document relevant details of each access event. Because manual processes make both the requestor and supervising party privy to password secrets, they depend on the trustworthiness and reporting diligence of the individuals in charge, thus reducing the reliability of any audit trail.



Automated Alternatives for Auditing and Alerting

Automated privileged identity management products such as ERPM can report the details of privileged accounts present on a wide range of devices, document access requests by individual, system and account, and show detailed diagnostic information that indicates which users are configured for privileged access to each resource.

The in-depth compliance reports provided by ERPM can help supervisory personnel investigate issues that can arise with systems, policies, and personnel to provide authoritative answers to such questions as:

- What individuals have requested access to a particular account credential, IT asset, or group of assets over a specified timeframe, and for what stated purpose?
- What resources has a particular individual attempted to access over a specified period of time, and for what purpose?
- What privileged accounts are present on a particular IT asset or group of assets?
- What users are configured to access privileged accounts, and at what level?

ERPM user activity reports are derived from comprehensive logs that document the date and time of each access request, the requestor and documented purpose, the success and failure of each operation, and the originating IP address of each request, as shown in Figure 8 below.

Manager	Account	Operation Description	IP Address	Operation Time	Result
LSC\CHRIS	(SXPP03)\SXPP03\Administrator	Password Recovery/Checkout - (SXPP03)\SXPP03\Administrator - Password check out - extended for (SXPP03)\SXPP03\Administrator	192.168.11.17	4/30/2009 9:05:31 AM	Success
LSC\CHRIS	(SXPP03)\SXPP03\Administrator	Password Recovery/Checkout - (SXPP03)\SXPP03\Administrator - Password check out - Comment:brad has installed a driver that may need to be uninstalled	192.168.11.17	4/30/2009 9:05:48 AM	Success
LSC\CHRIS	(SXPP03)\SXPP03\Administrator	Password Checkin - (SXPP03)\SXPP03\Administrator - Password check in - Comment:Uninstall Completed	192.168.11.17	4/30/2009 9:05:48 AM	Success
LSC\CHRIS	(SV02)\SV02\Administrator	Logon - Attempted Logon to LSC (Domain Controller: DCTR1)	192.168.11.17	4/30/2009 1:08:12 PM	Success
LSC\CHRIS	(SV02)\SV02\Administrator	Password Recovery/Checkout - (SV02)\SV02\Administrator - Password check out - Comment:ticket 4345	192.168.11.17	4/30/2009 1:08:40 PM	Success
LSC\CHRIS	(SV02)\Administrator	Password Checkin - SV02\Administrator - Password check in - Comment>Password checked in automatically as part of a password update job.	Local	4/30/2009 1:58:06 PM	Success
LSC\CHRIS	(S2KP01)\S2KP01\Administrator	Logon - Attempted Logon to LSC (Domain Controller: DCTR1)	192.168.11.17	4/30/2009 2:00:09 PM	Success
LSC\CHRIS	(S2KP01)\S2KP01\Administrator	Password Recovery/Checkout - (S2KP01)\S2KP01\Administrator - Password check out - Comment:rollback EX2	192.168.11.17	4/30/2009 2:00:45 PM	Success
LSC\CHRIS		Web Logout -	192.168.11.17	4/30/2009 2:02:04 PM	Success
LSC\CHRIS		Logon - Attempted Logon to LSC (Domain Controller: DCTR1)	192.168.11.17	5/5/2009 3:45:13 PM	Success
LSC\CHRIS	(SV02)\SV02\Administrator	Password Recovery/Checkout - (SV02)\SV02\Administrator - Password check out - Comment:configure MSJXC	192.168.11.17	5/5/2009 3:45:51 PM	Success
LSC\CHRIS		Logon - Attempted Logon to LSC (Domain Controller: DCTR1)	192.168.11.17	5/5/2009 4:15:11 PM	Success
LSC\CHRIS	(SV03)\SV03\Administrator	Password Recovery/Checkout - (SV03)\SV03\Administrator - Password check out - Comment:configure VRNT.DLL	192.168.11.17	5/5/2009 4:24:33 PM	Success

Figure 8 – ERPM Compliance Logs Show Activity Details for a Selected User

In addition to customizable auditing and reporting, ERPM provides configurable alerting that can be delivered by email or exported as SNMP (Simple Network Management Protocol) traps and triggers for frameworks like Microsoft Systems Center Operations Manager. Examples of alerted events can include successful and denied password checkout requests configured by platform and type, success and failures of password update operations, and process faults such as a failure to change passwords on systems that are offline.

Next Steps

Organizations that desire more insight into potential risks of the unsecured privileged accounts can contact Lieberman Software for an ERPM software trial. ERPM documents potential risks present in the infrastructure, enumerating 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.

Summary

News stories of supposedly compliant organizations that suffer costly data breaches and operational disruptions offer proof of the risks of ineffective privileged identity management. While it's possible to take control of privileged access using manual and ad-hoc steps, the recurring workload, potential security gaps and lack of an authoritative auditing trail can make manual remediation impractical for organizations with significant numbers of IT assets or more than a few personnel who may require privileged access.

Automated privileged identity management solutions such as Enterprise Random Password Manager from Lieberman Software Corporation can improve security and operational efficiency by discovering the presence of privileged accounts and their interdependencies on a wide range of hardware devices, applications and services. ERPM leverages a configurable choice of directory services and optional two-factor authentication to ensure that access is provided only to intended individuals. It hardens and auto-propagates login credentials wherever they may reside and provides a reliable audit trail to document the requestors, systems and accounts, timeframes, and purpose of each access request. ERPM provides IT personnel the automation necessary to ensure that the organization's security policies are efficiently put into practice.

About Lieberman Software

Lieberman Software Corporation, established in 1978 as a software consultancy, has been a profitable, management-owned organization since its inception. Lieberman Software pioneered privileged account password management software, releasing its first product to this market in 1999. Since that time, the company has continuously updated and expanded its solutions while growing its customer base to include many of the world's most secure enterprises.

Lieberman Software is a Microsoft Gold Certified Partner and has technical partnerships with such other industry leaders as Cisco, Novell, Red Hat, Hewlett-Packard, IBM, RSA and Intel. The company is headquartered in Los Angeles, CA, and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States.

For more information, visit www.liebsoft.com
or call 800-829-6263 (USA and Canada) or 01-310-550-8575 (International).