Privileged Identity Management

A Technical Overview
# Privileged Identity Management

## Contents

- **Introduction** .......................................................... 3
- Privileged Account Password Management Challenges ................. 3
  - Lack of Controls vs. Manual and Automated Methods ............... 4
- **System Architecture** .................................................. 4
  - Database ........................................................................ 5
  - Business Continuity and Disaster Recovery ......................... 5
  - Performance and Scalability ........................................... 5
- Discovery of Systems, Accounts and Services ......................... 6
  - Managed Targets .......................................................... 6
  - Discovery Techniques .................................................... 7
- **Password Management** .................................................. 8
  - Password Change Policies .............................................. 8
  - Password Change Jobs .................................................. 8
  - Password Encryption ..................................................... 9
- **Access Management** ..................................................... 9
  - Directory Authentication ............................................... 9
  - Multi-factor Authentication ........................................... 10
- **Workflows** .................................................................. 10
  - Help Desk Integration .................................................. 10
  - Usability ....................................................................... 11
- **Auditing** .................................................................... 11
  - Alerting and Integration ................................................ 11
  - SIEM Integration ........................................................... 12
- **Reporting** ................................................................. 12
  - Reporting Architecture ................................................ 12
  - Compliance Reports ...................................................... 12
  - Operational and Business Intelligence ............................... 13
- **Ease of Deployment and Operation** ................................. 13
  - Configuration vs. Customization ..................................... 14
  - Implementation Plan & Project Timetable .......................... 14
  - Proof of Concept .......................................................... 14
  - SDK .......................................................................... 15
- **About Enterprise Random Password Manager** .................... 16
Introduction

As a software vendor, we are seeing an increase in the number of Request for Proposals (RFPs) for Privileged Identity Management (PIM) solutions. Organizations want to automate the management of their privileged credentials – including root, admin, SYS, sa, and others – because these “Keys to the Kingdom” require special care and management. Manual efforts are not able to keep up with the growing number of privileged accounts in virtual environments, on network devices, in applications and of course, on systems.

Corporate governance requirements, private sector and government security regulations, and the need to eliminate what cyber security experts call “a top threat” has led to IT organizations rapidly adopting PIM controls.

This guide is based on the real-world requirements of organizations researching and deploying PIM solutions globally. It’s based on our experience working with customers who have compared us to other vendors in this space. This guide is not a complete requirements list; rather, it reflects the key functional and technical requirements you should consider in your evaluation of PIM solutions.

Note: This is a companion piece to our Privileged Identity Management Executive Overview.

Privileged Account Password Management Challenges

Your IT staff faces a complex set of obstacles to get privileged accounts under control because enterprise networks are constantly changing and user roles within your organization are frequently in flux. There’s usually no set of rules governing privileged credentials that control access to your applications, computer operating systems, databases, and network devices.

To comply with industry mandates such as SOX, PCI-DSS, HIPAA, FISMA, BASEL III and others – and to align with your organization’s internal controls – your IT staff must secure privileged accounts and monitor their use. Specifically, on an ongoing basis, you will need to:

- Detect and track all privileged identities present on a dynamic network
- Document and secure service and application account passwords
- Change each of these passwords on a set schedule, without disrupting other IT services
- Ensure dynamic segregation of duties so that only designated staff can access privileged accounts, at configured times, with the least privileged required to complete their work
- Audit user access to privileged logins to ensure that corporate and regulatory requirements are met
- Change privileged account passwords immediately after use to prevent sharing and reuse
Lack of Controls vs. Manual and Automated Methods

The principal methods of recording privileged passwords in most organizations include Post-It notes, print-outs left in the open, verbal or emailed shared passwords, and spreadsheets that list the passwords used by the Help Desk and others. In many cases, the spreadsheets and password files are kept on network file shares with minimal, if any, restrictions. Rarely is there any auditing of access to this data, yet even the most lax IT auditors will point out that uncontrolled access to sensitive data such as root passwords carries enormous risks, and the IT department should immediately take steps to address the problem.

Many organizations start by using manual and ad-hoc processes to manage privileged accounts. Without automation, however, full discovery and management of these credentials is nearly impossible to achieve. In the long run, manual methods usually prove to be cost prohibitive because:

- Writing, maintaining and troubleshooting scripts and manual procedures takes IT staff time away from more strategic projects.
- Failure to account for every privileged account leads to vulnerabilities that are easy for modern hacker tools to exploit.
- It is extremely difficult to locate everywhere privileged accounts are in use and then successfully change the passwords in all referenced locations.

Absent adequate documentation, logging, and failover design, the errors that can be introduced by ad-hoc processes are almost certain to cause costly IT service downtime that impacts large numbers of systems and users.

System Architecture

This section provides an overview of the basic architectural requirements for an automated privileged account management solution. Look for a solution that offers a system architecture that can accommodate the many changes that occur on your network over time. The solution should automatically:

- Detect and secure every one of your current hardware and software assets
- Have the flexibility to handle not only mainstream hardware and applications, but also the legacy and in-house applications that you support
- Handle changes on your network – including frequent changes in systems, network devices, applications, and users – with an absolute minimum of staff intervention and outside support

“It’s like painting the Golden Gate Bridge, starting at one end, working your way to the other end, and then starting over. Essentially by the time you were done changing service account passwords you would have to start all over all again.”

— IS Analyst
Large Federal Credit Union
• Scale to far beyond your lab environment – meeting the current and future management needs of your entire network
• Avoid the use of added endpoint agents that can increase your support burden and drain system resources

Database

Privileged account passwords should be stored and encrypted in a backend database. The performance and reliability of your PIM solution depends on its database platform. Choosing an industry-standard database can help lower your ongoing costs, since use of a database that is widely adopted and well documented makes it easy for IT staff to configure, secure and maintain the PIM solution as a whole.

Broadly-available, commercial databases like SQL Server and Oracle give your staff a choice of several cost-effective alternatives to configure for high-availability and recovery. Use of these well-documented database designs eliminates “security by obscurity,” assuring that IT personnel have all the information needed to keep the application and network secure while giving you options to deploy the latest in encryption solutions such as PKCS#11 and others. And, these open databases give you the choice to maintain your PIM solution with your own in-house personnel.

Business Continuity and Disaster Recovery

Because your PIM software controls access to the organization’s most sensitive accounts, it’s important to configure the solution for business continuity and disaster recovery.

Look for a solution that can support clustered and mirrored deployments for higher availability. Choose a deployment option that can support reliable database failover, and a PIM software architecture that minimizes single points of failure: for example, in a distributed environment if the system hosting the PIM administrator function were to go offline, it should still be possible for users to gain access to passwords. Above all, look for a PIM product that fully documents the mechanisms that it uses – and the options you can deploy – to assure reliable operation.

Performance and Scalability

Not all organizations deploy PIM to manage many thousands of systems across multiple geographies. However, the ability of your PIM software to scale economically from a few departments to a global network can provide enormous cost savings should your organization grow or your business needs change. Further, the performance of your PIM solution should not be impacted the more you grow.

A multi-threaded application is ideal, since this is a prerequisite for changing the thousands of passwords that are likely to be present on numerous machines within a reasonable about of time. The solution should also enable you to execute simultaneous requests with no performance degradation; for example, the processing time for 300 concurrent requests should be less than 10 seconds.

“If we follow every vendor’s desire to load agents, eventually all of our servers will be bogged down with the sole purpose of supporting those vendors’ products.”

— CIO
Major Television Network
To assure that your future needs will be met, choose an architecture that can easily scale up for performance and scale out for reliability and fail-over. When evaluating the scalability of your PIM solution, look for:

- An n-tiered architecture that gives you the option to deploy the password database, management console, web server and reporting database on separate machines
- The capability to deploy individual zone processors on remote machines to reliably handle password changes at distant locations and on isolated (DMZ) networks
- A console design and password change architecture – including a scalable back-end database and highly tuned, multi-threaded password change algorithm – that provides responsive console interaction and reporting even when processing very large password change jobs
- An architecture that supports network load balancing and clustering technology

**Discovery of Systems, Accounts and Services**

Any PIM solution that fails to discover substantially all of your privileged accounts can quickly overburden IT staff and lead to surprisingly expensive professional services contracts. Perhaps more importantly, lapses in coverage that leave individual accounts exposed – including privileged logins present in newly-deployed hardware and applications, legacy software, developer “back doors,” undiscovered services or any other type of IT asset – can make your network vulnerable to today’s sophisticated hacking techniques.

Examples of the key management targets that should be covered by any PIM solution are detailed below.

**Managed Targets**

In choosing a PIM solution look for explicit coverage of your present-day devices and applications, as well as a comprehensive list of popular management targets to help “future-proof” your purchase. In particular, look for a solution that can reliably discover and change the widest range of privileged accounts out-of-the-box:

- **Windows accounts** such as named accounts, built-in administrator and guest
- **Database accounts** such as Microsoft SQL Server, Oracle, DB2, MySQL and Sybase logins

“Not knowing all the dependencies of where a privileged account was used could cause cascading failures resulting in anything from inconvenience to outages the day after password changes were implemented.”

— Manager IS Security, Wings Financial
• **Midrange and mainframe accounts** on Linux, UNIX, OpenVMS, OS/390, OSX and TN3270

• **Network devices’ privileged logins** on Cisco, Foundry, HP, Juniper, NetApp and others

• Privileged logins on **out-of-band server management cards** found on HP, Dell, and other IPMI compliant servers

• **Active Directory** and **LDAP-Compliant** directory services accounts

• Privileged accounts used in web services such as **ASP.NET** config files and **SharePoint**; and in middleware tiers such as Oracle WebLogic, IBM WebSphere, and SAP NetWeaver

• **Interdependent process and service accounts in clustered environments** that must be thoroughly discovered and properly changed to avoid service disruptions

• **Shared account passwords** that would be otherwise maintained in employees’ spreadsheets and data files

Vendors that offer more comprehensive, out-of-the-box coverage as part of their core PIM offering, without the need for customization and added-cost services, provide better assurance that their solution is architected for good adaptability and will continue to support an expanding list of targets with each new release.

**Discovery Techniques**

PIM solutions that accommodate a broad range of system and account discovery techniques give you the flexibility to configure the solution once, with a minimum of interaction thereafter. Look for a solution that adds and then automatically tracks systems found in:

• Domain systems lists

• Network browse lists

• Active Directory/Other LDAP-Compliant Directories

• Scanned IP address ranges

• ODBC query results from configuration management databases (CMDBs) and other sources

In addition, the solution should make it easy for you to bulk-import system lists from text files, and to make ad-hoc entries through a management console.
Password Management

Regulatory mandates like PCI DSS, SOX, FISMA and HIPAA and standards like ISO/IEC 27002, COBIT and BASEL III give explicit guidance about password complexity, reuse, age, and other requirements. As a result, your corporate policies probably require you to enforce these rules when it comes to your privileged accounts.

Password Change Policies

PIM solutions provide the option to change passwords to static values that you choose, or to random values that meet the general conditions you set. In the case of random values – typically needed to comply with corporate policy or regulatory mandates – there should be easy-to-configure settings that specify password length, the use of special characters, upper or lower case letters, numbers, and so on.

It’s important to note that different management targets – including hardware, databases, and applications – can have different requirements for allowable passwords. It’s essential for your PIM solution to accommodate these differences and make it easy to choose the right settings wherever possible. Your PIM software should also support logical grouping of target systems so that it’s easy to configure specific policies for different types of target systems and account types – for example, NT compatible passwords for older lab gear, compliance with default Windows Vista/2008 password filter strings for newer hardware, etc.

There is one area of password management that is lacking in many PIM solutions: reliable password correlation and propagation. A distinctive capability of any sustainable PIM solution is the dynamic discovery of every location throughout the environment where a privileged account is being used or referenced. This is especially critical for privileged credentials like service and process accounts. Your PIM software should be able to propagate password changes to relevant targets across your network to avoid the potential for service disruptions and lockouts whenever changes are made.

Password Change Jobs

A PIM solution should make it easy for you to schedule password changes that are needed to that comply with your organization’s policies. And, the PIM product should properly handle exceptions (in the event of a network issue or if a target system goes offline) so that any failed password changes are reported and addressed.

A PIM architecture that organizes password change jobs by systems (as opposed to accounts) allows you to update the same account on multiple machines with a single job, and can make it possible to manage all of your password changes with the least effort. Once password change jobs are created, the PIM solution should process password changes without operator intervention.

PIM software should also have the capability to reset individual passwords or groups of passwords on-demand, and to schedule automated checks to ensure that each password stored in the database correctly matches the current login for each target account.
Password Encryption

PIM software encrypts passwords in a backend database. Encryption options should include military-grade AES encryption, a FIPS 140-2 software encryption module, higher levels of FIPS 140-2 compliance, and support for Hardware Security Modules (HSMs) that use PKCS#11. The PIM solution should also provide for SSL encryption between its distributed modules, and between the web application and user machines, to protect passwords and other sensitive information.

Access Management

The foundation of any good PIM solution is role-based access controls that map user roles (as defined by your directory services, in combination with rules you set inside the PIM product) to groups of approved IT resources – again, as defined by a combination of directory objects, discovery rules, and groups that you configure in the PIM solution.

Your PIM access rules can closely mirror your organization’s policies. They should update in real time whenever changes occur in your directory, and they can immediately alert you to activities that warrant your attention. For example, you can configure an explicit account inside your PIM solution for subcontractor personnel, without providing these outside employees with domain credentials – allowing your subcontractors to access a small subset of your systems. Further, you should be able to grant access through a Remote Desktop / SSH connection that does not disclose any passwords. You should also have the option to grant staff immediate, audited access to a particular group of servers or require departments or individuals (e.g., help desk staff, contractors) to get explicit management approval before access is allowed.

Directory Authentication

Your PIM solution should authenticate in real time with trusted Windows domains, popular standards-based directories such as Oracle Internet Directory and Novell eDirectory, and other LDAP and RADIUS servers. The PIM product should also provide you the flexibility to grant access to members of Windows groups, individual Windows users, roles (as defined by your directory services), RADIUS users, or independent, explicit user logins that you configure in the product.

As noted above, the PIM solution should allow you to grant each role the ability to access all resources, groups of systems and accounts that you define, or individual systems or accounts. Because you can typically create multiple levels of delegation within the PIM product, your best practice is usually to make permissions that are applied at the global level more restrictive, while granting broader permissions in rules that apply, say, to explicit accounts being recovered.

As noted above, PIM solutions allow for time-bound password retrieval that can force check-in and a password change after each access. This is critical for answering the question of “who had access at what time” and is the foundation for reliable logging and auditing controls.
Multi-factor Authentication

Because of the danger that could occur should highly-privileged accounts fall into the wrong hands, many of today’s regulatory mandates (including the Consensus Audit Guidelines and others) require individuals to use multi-factor authentication when they request access. Look for your PIM solution to support all of the time-based and event-based methods that your organization might adopt, including:

- Out-of-band, Time-based One-Time Password (TOTP) authentication by email and SMS using OATH services – providing easily configured multi-factor security that requires nothing further for your organization to buy
- OATH authentication using third-party tokens
- Out-of-the box support for proprietary tokens including RSA SecurID and YubiKey
- PhoneFactor Phone-based Authentication
- SafeNet Multi-factor Authentication
- RADIUS Multi-factor Authentication

Use of multi-factor authentication can help safeguard your organization from common hacker exploits. For example, an organization that recently fell victim to a hacker posing as an executive (who tricked an administrator into disclosing a highly privileged server login) could have prevented data loss by deploying inexpensive out-of-band multi-factor authentication using email or SMS delivered to IT staff cell phones.

Workflows

Your PIM solution should make it easy to configure workflows that quickly provide authorized users audited access to privileged logins, from any allowed location, at approved times, while automating the approval steps to save IT managers’ time.

The solution should allow you to configure checkout rules for each user role. For example, for a group of critical servers you might want to be notified if a specific IT manager requests access, but require all other personnel to get explicit approval before gaining access. Workflow capabilities should allow for users to request access and for managers to grant access within the system in a user-friendly manner.

Help Desk Integration

Well-integrated PIM solutions work in concert with your Help Desk software to augment security and save staff time. Help Desk integration should help you verify that all privileged password check-out requests originate from valid trouble tickets, assure that all requestors have been configured for the requested level of privileged access, and automatically update trouble tickets to reflect activity within the PIM product. PIM solutions should also be able to create Help Desk tickets from within the product when unexpected events such as failed logins occur.
Look for your PIM solution to support major Help Desk systems such as HP Service Manager, BMC Remedy, Microsoft System Center Service Manager, ServiceNow and others – and to efficiently integrate with those vendors’ supporting frameworks including CMDBs and SIEM systems.

**Usability**

Your PIM solution should help to raise the productivity of IT staff, Help Desk personnel, and anyone else who uses the product to access privileged accounts for routine administrative duties and emergency repairs. To accomplish this goal the software should have an intuitive user interface and be able to:

- Quickly authenticate users with their domain logins or other credentials
- Present privileged passwords to authorized personnel in as few as two clicks after they login
- Allow access from anywhere that you allow, in an encrypted Web session
- Provide different views and options depending on the user’s role – for example, displaying only those systems and accounts configured for access to each end-user, and presenting delegation and reporting features only to those administrators who are allowed access
- Present systems and accounts in ways that make it easy for users to drill down to the resources they want to access – for example, by presenting hierarchical views, sort-able lists, filters, and so on
- Make it easy for contractors and others who may not have domain logins to access the solution

**Auditing**

Reliable auditing coverage is critical to any PIM solution, so the software should support a variety of methods to record and audit any action that it performs. This should include text-based application logs, an internal auditing database, application Syslogs, email notifications, and integration with outside frameworks using traps for SNMP, Triggers for Microsoft System Center Operations Manager, and so on.

The system should record access to the Web console for password requests, approvals and check-out, delegation changes, reporting and other activities, access to its management console for configuration and reporting, and all password change job activity.

**Alerting and Integration**

The goal of your PIM alerting features is to allow you and others to take appropriate action when important events occur. The solution should be configurable so that events can trigger email alerts, run specific programs, and communicate with trouble ticketing applications, SIEM solutions, and other frameworks. The solution should also be capable of alerting on actions such as password requests and check-outs, password changes, failed password change jobs, console and web application activities, and the like.
In addition to out-of-the-box integration with popular Help Desk and SIEM frameworks, look for the solution to provide an easily configurable process for integrating with virtually any Help Desk system, provisioning database, security framework and other important applications. Integrations that are not provided out-of-the-box should not require extensive professional services; rather, your own personnel should be able to easily and quickly configure these integrations with a minimum of effort.

**SIEM Integration**

By themselves, SIEM applications lack the ability to correlate security events with human and automated actions that use privileged credentials. For this reason the integration of your PIM solution and your SIEM framework can close a critical blind spot in your security framework by tying individuals and processes that have privileged access to the security events that they can trigger.

Out-of-the-box integration with leading SIEM frameworks such as HP ArcSight ESM™, RSA enVision™, and Q1 Labs QRadar™ is an important consideration when choosing a PIM solution, as is the ability to easily integrate with other platforms.

**Reporting**

Your PIM solution should supply a range of preconfigured reports that help you monitor the performance of the application, ensure that security and compliance goals are being met, and provide business intelligence to assist with your daily operations. The solution should also allow you to create custom reports using popular third-party reporting tools such as Crystal Reports™ and SQL Server Reporting Services.

**Reporting Architecture**

Use of a separate data warehouse – whether configured as an additional database on the same server as the PIM solution or as a database on a different machine – can help assure responsive reporting regardless of the complexity of the report or the size of the PIM installation. By configuring a separate data warehouse you can assure that archival, data segmentation, replication and reporting data growth can be more easily accommodated over time. More importantly, a data warehouse model allows for structured, minable data that remains completely segmented from encrypted account passwords.

**Compliance Reports**

Your PIM solution should provide preconfigured reports that make it easier to prove compliance with regulatory mandates such as SOX, PCI-DSS, HIPAA, CAG-12, BASEL III and many others. The PIM application should allow ad-hoc reporting and the collection of reporting data according to schedules that you define.
Authorized personnel should have access to these reports through both the administrator console and the application web client. Reports that present the PIM solution’s activities as a whole are often used for compliance reporting. These can include reports of all systems that are managed and unmanaged, reports of stored passwords and their status, reports of all password change jobs, reports that show activities by selected users, and reports that show activity for selected systems or accounts.

**Operational and Business Intelligence**

Your PIM solution should provide the reports you need to meet your compliance requirements, plus give you other actionable business intelligence. You can gain business insight from reports that tell you about password requests, password check in and check out, delegation change requests and others. Taken together with information from preconfigured compliance reports, your PIM solution should be able to answer questions such as:

- What were an employee’s actions in the 30 days before he left his job?
- Which of our systems had the most administrative login activity over the last 30 days?
- Which of our systems have highly privileged, orphaned accounts that may be present because of personnel changes or other activity?
- Which of our systems have privileged accounts that may use vulnerable, default logins?

**Ease of Deployment and Operation**

Most organizations can’t justify spending months of personnel time and vast sums in professional services fees to deploy a PIM solution. You should be able to deploy well-designed PIM software in a matter of days, with a minimum of outside assistance.

Further, your ongoing management burden for the PIM solution should be minimal. The operation of your PIM software should be self sustaining, requiring minimal administrative involvement. Ease of deployment and manageability should be your key considerations for choosing the right PIM solution to manage a dynamic environment. We’ve heard stories of customers who weren’t able to make some vendors’ solutions operational – even after taking months of effort and paying vendor professional services fees that far exceeded the original software cost.
Configuration vs. Customization

Look for a PIM solution that is easy to configure. Expect drop-down menus and dialog boxes to enable easy configuration at all places in the product. You should receive the same vendor-supported code base as every other customer and be able to simply configure the solution for your specific purposes, however complex. You should not have to customize your PIM solution as a one-off implementation since this could multiply your future costs and complexity of updates and security fixes; and, configuration should not require expensive professional services. Again, expect your PIM solution to be deployed and configured in hours or days, not months.

To assure that your organization achieves a positive return on its software investment, look for a PIM vendor who can provide references with deployments that are similar in size to your own, along with:

- A detailed, written analysis of your organization’s business goals
- Detailed documentation of your needs with respect to systems, applications, and lines of control
- A statement of work that details the time and cost required to bring unsecured privileged accounts present in your target systems and applications under control, including full disclosure of all back-end services costs

Implementation Plan & Project Timetable

Your PIM vendor should provide a firm cost proposal and definitive, realistic project timelines for your implementation services. These services can include any specialized preparation of your host systems and network environment needed for the deployment, configuration of disaster recovery and high availability options, planning and configuring workflow and role-based access controls to align with your organization, and help to create any specialized reports that may be needed to meet compliance or operational objectives.

In all cases you should expect your full project to be completed – and the PIM solution securing all of your required management targets – within a few weeks.

Proof of Concept

As part of your selection process you should expect that your PIM software vendor provide a proof of concept that covers all of your hardware platforms and a realistic sampling of your essential applications. For each platform and application document what capabilities your staff can deploy unassisted out-of-the-box, what capabilities need a vendor’s professional services personnel to accomplish, and what capabilities aren’t delivered at all.
As you proceed with your evaluation be aware that marketing checkboxes often lie. Craftily written marketing pieces can suggest that a product’s capabilities with respect to one target platform, application or deployment scenario extend to all areas where the vendor claims coverage, and salespeople often believe their organization’s own hype.

Ask very explicit questions – both of vendor engineers and reference customers – about how individual target platforms, managed applications and use case scenarios are configured and deployed. In each case was the vendor’s capability delivered out-of-the-box, only through custom development, or never at all?

**SDK**

Because every IT environment is different, an important consideration is the ability of your PIM solution to manage and operate reliably with the systems, applications and devices that are unique to your enterprise. Your PIM solution should offer a Software Development Kit (SDK) that can address corner cases, with APIs available for virtually all platforms to allow real-time, programmatic access to passwords. The SDK will allow applications and individuals to access the password store independently of the product’s original interface. Key use cases include:

- Improving the security of your in-house applications and scripts by configuring them to retrieve privileged credentials on demand rather than embedding the passwords where they can be easily compromised
- Programmatically updating account information in the password store
- Programmatically enrolling systems in the PIM without waiting for dynamic group updates
- Replacing clear-text passwords embedded into applications with secured retrieval from the encrypted database

**Maintainability**

Look for a PIM solution with open documentation – accessible to everyone online. To save long-term costs for your organization the solution should include product upgrades with your cost of support, and upgrades that install quickly, by your in-house staff, without the need to pay for additional professional services.
About Enterprise Random Password Manager

Enterprise Random Password Manager (ERPM) from Lieberman Software is the first privileged identity management solution that automatically discovers, secures, tracks and audits the privileged account passwords in the cross-platform enterprise.

Competing solutions cannot come close to what ERPM offers in terms of continuous auto-discovery of privileged accounts everywhere in the enterprise, password propagation and service account management. ERPM is far superior for supporting large, dynamic, complex environments; it automatically detects changes in the enterprise and immediately updates itself as systems and devices come on and off your network.

ERPM integrates out of the box – using only a few mouse clicks – with leading Help Desk software, SIEM frameworks, multi-factor authentication technologies, remote access devices and more.

ERPM customers deploy the solution on global networks in days – not months – to lower their cost of ownership and quickly boost IT staff productivity. After deployment, ERPM automatically keeps up with changes on complex, heterogeneous networks without customization, scripting, and added-cost professional services.

Next Steps

Organizations that want to learn more about automating privileged account security can contact Lieberman Software for an ERPM software trial. ERPM trial software is available at no cost to qualified organizations.

For more information, email ERPM@Liebsoft.com.