Gain Accountability and Control of Your Privileged Users with CA Privileged Identity Manager

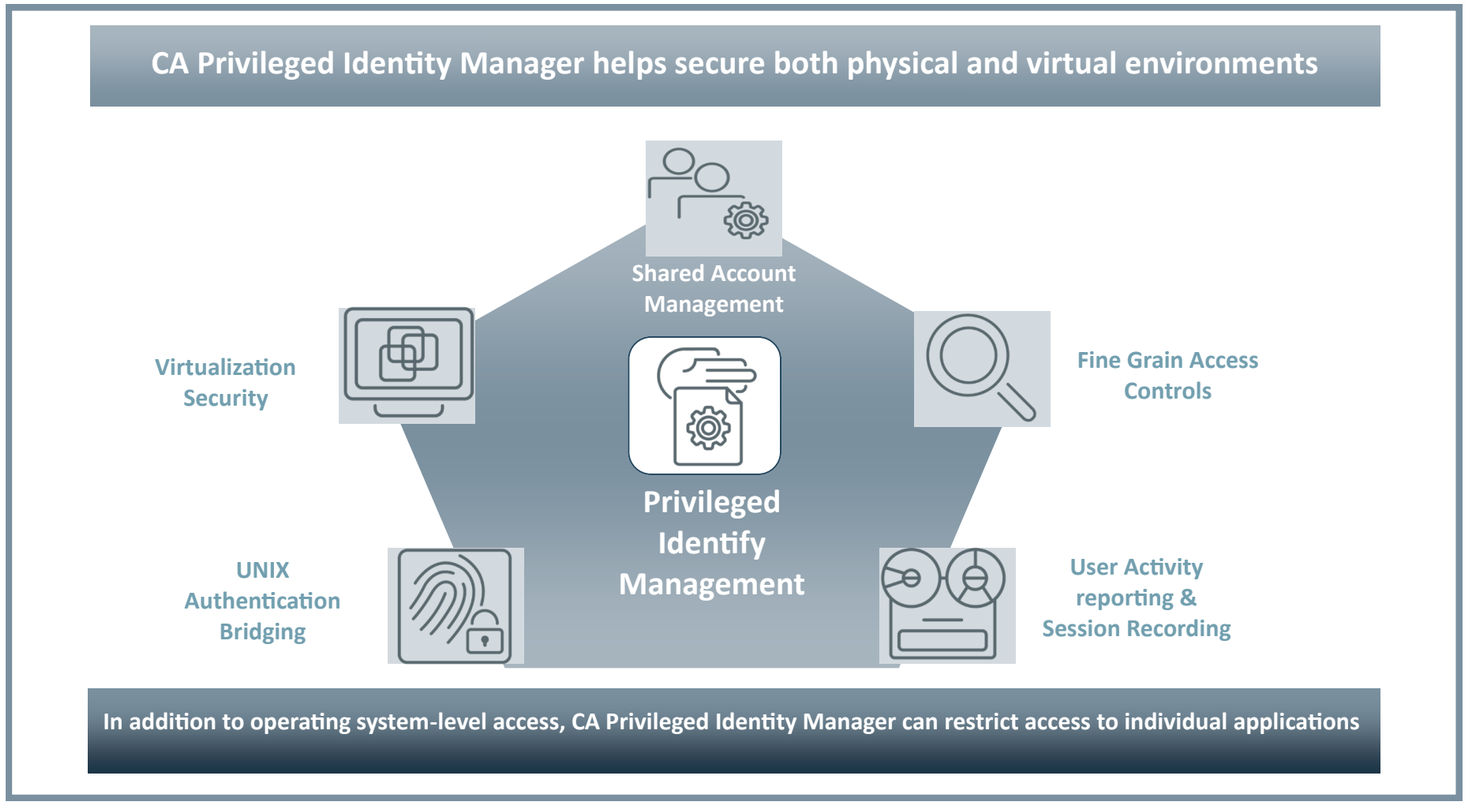
CA Privileged Identity Manager is a comprehensive and mature solution for privileged identity management (PIM) in both physical and virtual environments. CA Privileged Identity Manager is a scalable solution that is capable of providing shared account password management, fine-grained access controls, user activity session recording and UNIX authentication bridging across servers, applications and devices from a central management console. CA Privileged Identity Manager for Virtual Environments brings privileged identity management and security automation to virtual environments, from the infrastructure to the virtual machines.

Business challenges

Businesses are facing not only increasing security challenges, but complex regulatory requirements that require them to control the actions of privileged users—to manage their access to systems and be able to prove their ability to do so.

Failure to control privileged identities could result in data loss or destruction, malicious damage, fines, lawsuits and a loss in shareholder value. In addition, auditors are requiring their clients to proactively demonstrate that they have the ability to control privileged users and report on their activities.

Standards and requirements are also catching up with the risks associated with virtualization. The Payment Card Industry Security Standards Council (PCI SSC) updated its requirements to include virtualization with version 2.0 of its Data Security Standards and also released a separate informational supplement on virtualization guidelines.



Key features

- Shared account password management
- Virtualization-aware automation of security controls
- Fine-grained access controls
- UNIX authentication bridging
- User activity reporting
- Session recording
- Segregation of duties
- Hypervisor hardening
- Protection for Amazon Web Services (AWS)
- Supports two-factor authentication

Key benefits and results

- **Enable accountability for privileged users.** Control how privileged users access and use systems and data.
- **Secure both physical and virtual environments.** Control privileged identities on physical systems, virtual machines and the hypervisor.
- **Facilitate compliance.** Address requirements such as PCI and ISO 27002.

Marquee benefits yielding **$618** per year in savings are detailed on the reverse side of this document in order to show examples of business value achievable through this identity management approach

For more information, please visit **ca.com/securecenter**

ca technologies

Business Value Estimations

CA Privileged Identity Manager benefits can be quantified via a wide range of benefit scenarios. A selection of these is listed below to show common areas measured.

Business Value Proposition	Business Value Enabler	Specific Measurement	Solution Area	Impact [1] Range	Key Resources Affected	Average [2] Resource Value	Projected [3] Savings / year
Reduced cost for system administrators to fulfill user requests	The solution provides self-service capabilities that enable users to request access to privileged or shared accounts. In addition, the system can gather necessary approvals to grant access to these accounts	Savings in system administrator labor cost	Privileged Identity Management	20 - 30%	Administrator FTEs	4	$90,000
Reduction in Service Desk call through reduction in password reset calls	Self-service capabilities enable users to request access to privileged or shared accounts. The system can also gather necessary approvals and grant access to these accounts	Savings in Service Desk labor costs	Privileged Identity Management	20 - 30%	Administrator FTEs	5	$112,500
Reduction in operations costs for legacy PIM system	The solution provides the opportunity to retire legacy identity and/or role management systems, thereby avoiding any enhancement costs associated with these systems	Savings in labor costs for operations and support of legacy systems	Privileged Identity Management	90 - 100%	Software Developer FTEs	2	$304,000
Reduction in time for security policy and UNIX account administration	Reduction in time spent by system administrators manually performing account admin role through centralized management and automatic distribution of security policy changes. Active Directory for the management of UNIX accounts and users via the UNIX Authentication Bridge are leveraged	Savings in UNIX system administrator labor costs	Privileged Identity Management	30 - 40%	UNIX Administrator FTEs	2	$112,000

This table shows some **key benefits** of **CA Privileged Identity Manager**. Your CA Technologies representative can also share additional and more detailed ROI business case examples for this solution by engaging the CA Business Value Analytics Team. This team works with CA's customers to develop and analyze a comprehensive set of assumptions and environment specific metrics in order to build customized projective business cases.

1 The Impact Ranges shown above are estimations derived from the analysis of benchmark data which is a composite of data derived from industry analyst published information, interviews with subject matter experts and experiential data from prior projective analyses.

2 The **Average Resource** column metrics may be typical of large multi-national corporations offering diverse products and services to their customers. Productivity benefit calculations are based on metrics not shown such as # of users, frequency of user requests etc. For the sake of simplicity, they were made equivalent to the number of FTE's in tasks associated with the related benefits.

3 The **Projected Savings** calculations are based on the product of the midpoints of the Impact and Average Resources to show a single representative potential savings value. The labor rates for all FTEs are assumed to be $45/hour and $80/hour depending on required skills for a 2,000 hour work year. Please note, the values expressed in this table are not a guarantee of achievable results and will vary depending upon your current infrastructure, people, and processes as well as the appropriate, effective implementation, adoption, and use of the CA solution.