Control, Monitor and Audit Privileged User Accounts to Prevent Breaches and Power Your Business

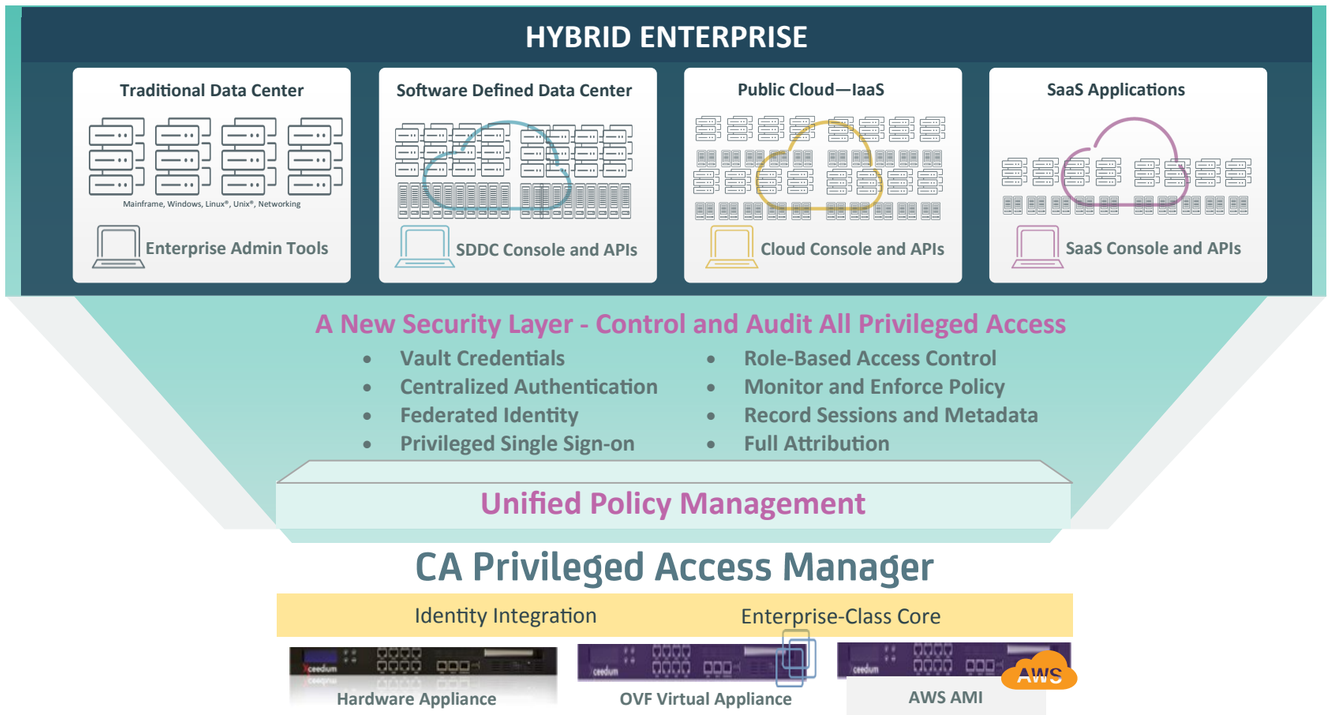
Quickly deployable and delivering fast time-to-protection, CA Privileged Access Manager is designed to secure all IT resources, facilitate compliance and minimize costs. Available as either a hardened hardware or virtual appliance, CA Privileged Access Manager is designed to prevent security breaches by consistently protecting sensitive administrative credentials, such as root and administrator passwords, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity across virtual, cloud and physical environments.

Business Challenges

- Many data breaches happen because of compromises in privileged user accounts. Standards and regulation bodies as well as auditors have recognized the risks associated with privileged users and have introduced regulatory changes and audit standards to mitigate these risks.
- Unfortunately, cobwebs of insecure legacy practices of administrators sharing passwords or embedding them in automation scripts are difficult to find, cleanup and prevent. Changing compliance requirements have further complicated this goal for total privileged user account management and make delaying appealing.
- But you cannot wait any longer. Risks are spreading like wildfire in growing dynamic and distributed virtualized and cloud environments common in enterprise IT today.
- One improperly authorized privileged account can cause widespread and irreparable damage to an organization's infrastructure, intellectual property and brand equity, leading to sudden drops in market value and broad organizational disruption.
- You need to cleanup your insecure legacy practices and technologies quickly with a proven privileged access management solution that works across all of your IT resources.

Marquee benefits yielding **$2.8M** 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

Privileged Account Management for the Hybrid Enterprise



Key Features

- Unify cross-platform support.
- Control access that is role-based and fine-grained.
- Get privileged user credential protection.
- Monitor, audit and record sessions.
- Support security and privacy regulations.
- Fully attribute activity to individuals.
- Manage password and keys.
- Get VMware, AWS, Linux®, UNIX®, Windows®, mainframes and network gear protection.
- Multifactor authentication, single sign-on, federation support.
- Achieve interoperability with Active Directory,
- LDAP, Radius, TACACS+ and other identity stores.
- Automatically discover virtual and cloud-based resources.

Key Benefits and Results

- Control privileged access across all IT resources.
- Manage privileged account credentials.
- Monitor, react and record everything.
- Protect hybrid-cloud consoles and management APIs.
- Provide for positive privileged user authentication.
- Prevent leapfrogging.
- Automatically discover and protect AWS and virtualized resources.

LOWER TCO!

An alternative product supports only **400** concurrent recorded user sessions per server, with a pair of load-balanced servers, for a total of 800 concurrent recorded sessions. Whereas a single CA Privilege Access Management appliance can support **2,000** (or more) recorded sessions - a 5 to 1 ratio!

A pair of CA Privilege Access Management appliances set up with load balancing would support 2,000 recorded sessions per appliance, for a total of 4,000 concurrent recorded sessions, or **five times more than the competition.**

For the competition to scale to the same 4,000 sessions as the pair of CA PAM appliances provides, you could be required to stand up 10 servers.

For more information, please visit

ca.com/Privileged Access Management

ca technologies

Business Value Estimations for CA Privileged Access Management

CA Privileged Access Management solution 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	Impact [1] Range	Key Resources Affected	Average [2] Resource Value	Projected [3] Savings / yr
BREACH PREVENTION Avoidance of Costs of Breach	CA Privileged Access Management (CA PAM) controls access to privileged account credentials and to protected devices using a zero-trust model, and rotates the privileged credentials according to customer policies. CA PAM ensures user accountability by auditing privileged activity and by recording videos of user sessions.	Reduction in the number and cost of successful security and data breach attacks	75-85%	Cost of data breach events @ $154 per lost or stolen record, and @ $170 per remediated record	3,450[4] compromised credentials	$894,240
BREACH PREVENTION Improvement in Revenue Protection	The growing awareness of identity theft and consumers' concerns about the security of their personal data following a breach ,has contributed to the increase in lost business. CA Privileged Access Management mitigates the data breach cost component which includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill.	Improvement in revenue protection	20-30%	Risk of compromised privileged access credentials	$1.57M[4]	$1,099,000
COMPLIANCE & AUDIT Reduction in External Auditor & Compliance Fees	Regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts. However, the time and cost involved in proving compliance with regulatory mandates can be enormous. CA Privileged Access Manager can help reduce the time required to prove adequate protection and management of passwords and monitoring of privileged users and accounts, thus reducing external auditor fees due to streamlined & automated remediation while achieving & maintaining standards compliance (PCI DSS,HIPAA,NERC-CIP,FISMA).	Reduction in audit finding fees and compliance penalties	40-60%	External audit costs	$4,000/issue[5] $110,000 non-compliance violation	$255,000
OPERATIONAL EFFICIENCY & PRODUCTIVITY Reduction in IT System Administrator Labor Costs	Automating password changes and the task of enforcing strong passwords as part of an organization's security best practices decreases both security and operational risks, while increasing staff productivity. With credential management features like automated or facilitated discovery, secure storage/vaulting, automated policy enforcement, secure retrieval and automated log-in, CA PAM can simplify and speed day-to-day tasks of providing authenticated privileged users with quick access to resources.	Reduction in system administrator labor cost	40-60%	Managed device accounts	50,000[6]	$156,250
REDUCED BUSINESS & IT COST FOR UNSCHEDULED OUTAGES Reduction in Unscheduled Outage Costs	Tightly controlling access and privileges in Hybrid Enterprise environments reduces the occurrences of unscheduled system downtime related to unintentional errors and malicious activity. Privileged users gain access only to authorized hybrid-cloud infrastructure, with all activity fully monitored and recorded.	Reduction in cost of downtime	30-50%	Outage costs	$1,358,800[7]	$271,760
EASE OF IMPLEMENTATION & SCALABILITY Reduced Implementation and Application Operating Costs vs. Competing Solution	CA Privileged Access Management is delivered as a single appliance which can be quickly deployed in hours as a hardened device or a virtual machine, protecting your enterprise resources with one scalable, agentless solution. A single appliance protects thousands of resources and also supports a larger number of concurrent sessions with fewer appliances, thus providing for a savings in IT labor costs as well as the avoidance of costs associated with the total cost of ownership (TCO) for servers and licenses, as result of solution configuration transparency.	Lower costs to implement & scale	75-85%	System administrator FTEs Total cost of ownership (TCO)	2 5 to 1 ratio	$130,000

This table shows some **key benefits** of **CA Privileged Access Manager.** Your CA Technologies representative may 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 Range and Average Resource Values to show a single representative potential savings value. The labor rates for FTEs are assumed to be $50 per hour for IT System Administrator skills and 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 appropriate, effective implementation, adoption, and use of the CA solution.
4. Calculation uses 23,000 exposed, 15% compromised, and data breach cost of $154/ lost or stolen record & remediation costs of $170/record as published by Ponemon Institute LLC in its 2015 Cost of Data Breach Study: Global Analysis.
5. External Audit FTE Fees used in calculation are $4,000 per issue with compliance Issue volume of 100 and annual cost of non-compliance violations of $110k.
6. Managed resource/device count of 10,000 is used in calculation with 5 accounts per device requiring 15 minutes of Sys tem Administration effort to provide or update privileged user access.
7. Calculation assumes one business interruption event per year, average downtime of 86 minutes, and uses an average Network Outage cost, of $7,900/min. to estimate cost of outage. Emerson-Ponemon-Cost-Unplanned-Data-Center-Outages 2013