**WHITE PAPER** | JUNE 2017

# Privileged Access Management: A Roadmap to Calculating Total Cost of Ownership

Uncovering the hidden costs and benefits of your PAM implementation approach

ca technologies

# Table of Contents

**Section 1:** 3
Introduction

**Section 2:** 3
Privileged Accounts Linked to High-Profile Breaches

**Section 3:** 4
Protecting Against Privileged Account Breaches with PAM

**Section 4:** 5
PAM Implementation Strategy Has a Major Impact on TCO

**Section 5:** 6
Building Blocks of a Comprehensive PAM Solution

**Section 6:** 6
Assessing the Business Impact of Comprehensive PAM to the Organization

**Section7:** 9
Bringing It All Together

**Section 8:** 10
Conclusion: A Long-Term View of TCO

### Section 1

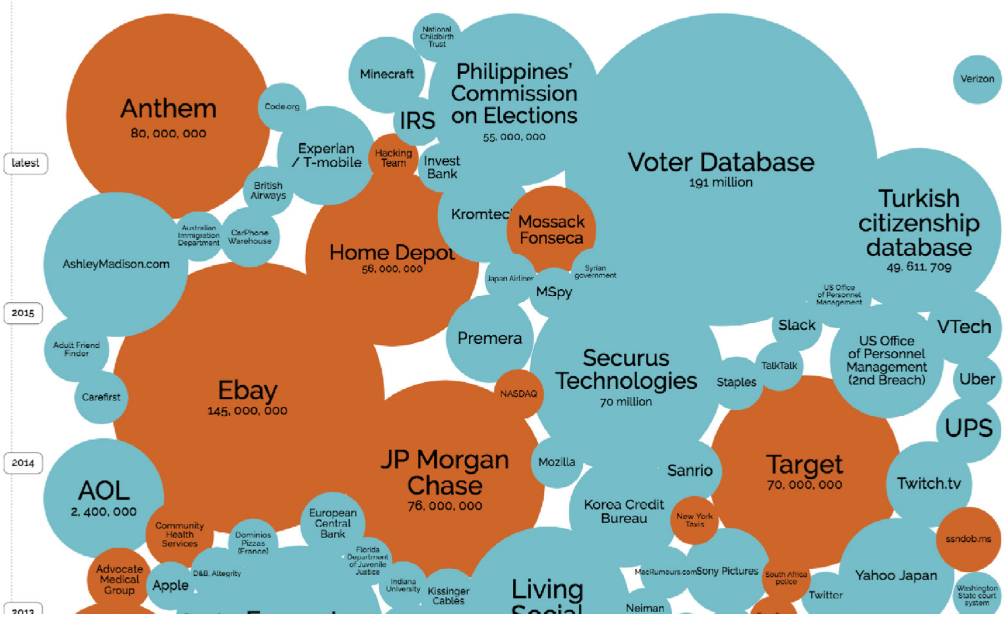
## Introduction

Privileged user accounts—whether usurped, abused or simply misused—are at the heart of most data breaches. Security teams are increasingly evaluating comprehensive privileged access management (PAM) solutions to avoid the damage that could be caused by a rogue user with elevated privileges, or a privileged user who is tired, stressed or simply makes a mistake. Pressure from executives and audit teams to reduce business exposure reinforces their effort, but comprehensive PAM solutions can incur hidden costs, depending on the implementation strategy adopted. With multiple capabilities including password vaults, session management and monitoring, and often user behavior analytics and threat intelligence, the way a PAM solution is implemented can have a major impact on the cost and the benefits. This report provides a blueprint for determining the direct, indirect and hidden costs of a PAM deployment over time.

### Section 2

## Privileged Accounts Linked to High-Profile Breaches

High-profile security breaches have become a constant element in the news, and experts say that between 80 and 100 percent of them involve use of privileged accounts. An escalating number of attacks involve the accounts of IT administrators, application developers, business managers, partners, suppliers and C-suite executives alike. Once the perpetrator is inside the system, he can move horizontally and vertically to access sensitive information and install malware to cause future damage. However, it's difficult for an IT administrator to determine whether there's a problem when privileged users access sensitive areas: This could be normal everyday activity.



The bottom line: the role of the privileged user can be the weakest link in the security chain for any organization, of any size, anywhere in the world. Addressing it properly can prove to be cost-effective for years to come.

**Section 3**

# Protecting Against Privileged Account Breaches with PAM

There are numerous aspects of information security, and privileged access management is just one of them. In general, organizations take a serious look at PAM for one of two reasons:

- They encounter a serious problem (e.g., they have been breached or have not met compliance requirements)
- They are ready to implement best practices

Regardless of the reason, it's not uncommon to make assumptions about implementation of a PAM solution. It may be tempting to take a short-term view, assuming that you can start with a limited set of functionalities and increase the scope and scale of the implementation over time. While this might be reasonable with some other security measures, experience shows it is neither technically nor financially practical with PAM. In fact, this is one area where it is extremely important to take a long-term view: devices, endpoints, users and accounts must be protected and compliance issues must be taken into account, as well as the company's roadmap. All of these factors will impact the total cost of ownership.

## Devices

We are no longer tasked with just protecting traditional endpoints. Today, the scope has broadened to encompass virtualized environments, containers and cloud-based systems. Hybrid IT infrastructure, management consoles, large numbers of resources and constant change can expand the available attack surface.  Adequate protection requires defenses that incorporate your entire environment from the beginning so that you can provide the breadth and depth of protection commensurate with the threats. Future needs such as these must be factored in when planning a PAM implementation.

## Users

Phishing and social engineering are now commonplace methods for obtaining privileged user credentials. Outsider threat (and increasingly prevalent insider threat) calls for full contextual information: We need to understand normal privileged user behavior so we can isolate the abnormal. The very concept of a privileged user is changing with the adoption of cloud, hybrid and agile development methodologies: For example, line of business owners may be assigned administrative privileges for cloud-based CRM solutions. Complicating matters further, user behavior changes over time and targeted attacks morph, making it difficult to tell with certainty whether an account has been compromised. Privileged user management solutions need to continuously learn and improve so they can identify potential breaches.

## Compliance

A constant requirement for organizations of any size, staying compliant (and proving it) can quickly lead to "regulatory fatigue" due to the sheer volume and scope of regulatory change.

PAM technologies need to support regulations governing the controls and processes used to ensure cyber security. This might include documenting access to configuration settings and private data, enforcing ITIL®, and providing definitive audit trails for the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS) and other regulations. Proof of compliance needs to be built in from the start, not bolted on as an afterthought.

**Section 4**

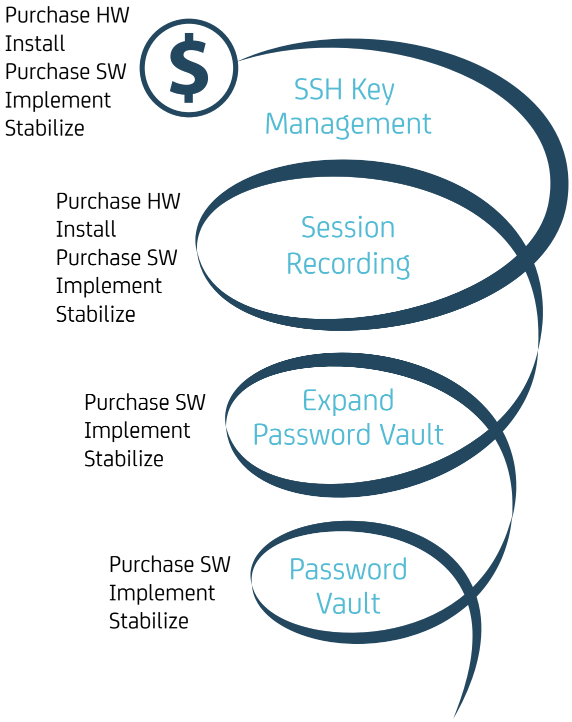
## PAM Implementation Strategy Has a Major Impact on TCO

The implementation method chosen for a PAM solution will have a major impact on the total cost of ownership. It's important to understand the two methods of implementing a PAM.

The first (we'll call it "comprehensive") is to build a roadmap of the key requirements, procure a product that provides all the capabilities—including future requirements—up front and then grow the scale and scope of capabilities over time, in stages. As an example, if you need password vaulting, session recording and secure shell (SSH) key management, you can purchase a product that incorporates all of them and turn on capabilities as they are needed. All are integrated, and there is no need for a long stabilization period.

The second (which we'll call "piecemeal") also starts with a roadmap, but products are procured as they are needed. For example, if the roadmap includes the same three capabilities as before, you can buy the password vault first, and after implementing it and stabilizing it over a period of months, you can go back to the vendor and buy session recording (and any necessary additional hardware), implement and stabilize it over six months, and then do the same with SSH key management.

The method chosen can affect both TCO and time to value. Implementing a comprehensive integrated PAM solution built on intelligence-gathering features can provide both faster time to value and lower TCO. The costs are known and predictable. In contrast, when the implementation is piecemeal, the initial deployment may be simple: a password vault for just a few accounts, which grows over time by increasing the number of accounts in the vault, and later adding session recording. However, the costs become unpredictable because infrastructure costs may vary with each added module. In addition, the customer is locked into the vendor, which may not be optimal for the customer. TCO calculations must take into account the cost, time and exposure resulting from adding scale and scope in a piecemeal implementation. Costs include both tangible (the cost of licenses, infrastructure and the like) and intangible, which includes time-to-value, prolonged exposure to risk, integration and maintenance costs, and others. Scripting and maintenance for adding additional endpoints for password vaulting may, for instance, be very different from what is needed for SSH key management.



To get a better idea of which questions to ask and capabilities to evaluate, it helps to understand what makes up a comprehensive PAM solution and how to determine the qualitative and quantitative benefits versus the financial cost.

Section 5

## Building Blocks of a Comprehensive PAM Solution

A comprehensive PAM solution has several core components, including the ability to control privileged access across all resources, secure storage of privileged credentials, monitor and record activity, protect hybrid cloud consoles and management APIs, and analyze user behavior to detect anomalies that might be indicators of compromise. Some specifics to keep in mind when evaluating PAM:

**Password vault.** A hardened and encrypted password vault or safe for storing credentials manages passwords and other credentials or tokens by changing them at configurable intervals, per policy. This helps protect administrative, shared and service accounts, as well as application-to-application accounts and hybrid cloud environments. However, password vaulting by itself is not enough.

**Session monitoring.** This vital component is often "missing in action" in an initial piecemeal deployment. The ability to automatically initiate a remote session that records, analyzes and monitors a privileged user session allows for real-time monitoring and post-session analysis. This capability should not be added after the fact: When a privileged user violates a policy or otherwise exhibits anomalous behavior, you want to start monitoring immediately, not six months from now.

**Hybrid environments.** A comprehensive PAM solution can control privileged access to cloud resources, virtual machines and hypervisors, in addition to traditional physical data center environments. Automatic discovery is key, since new resources can be added to the environment in minutes.

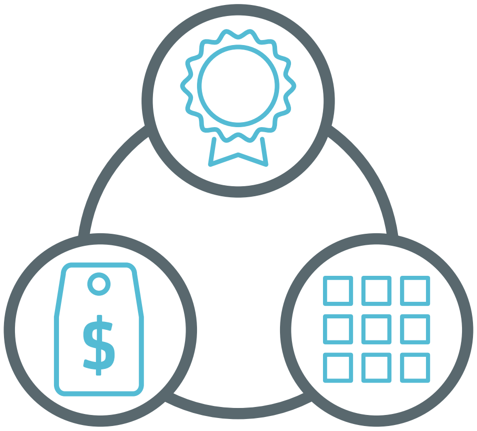
**User behavior analytics.** A comprehensive PAM solution can distinguish abnormal from normal privileged user behavior and trigger additional protection mechanisms when anomalies are seen. It collects domain-specific, contextual data and performs advanced analytics to build risk models based on previous behavior patterns. When It sees unusual behavior, it can automatically trigger additional authentication (such as Radius, TACACS+ or CA Advanced Authentication) or a session recording.

A comprehensive PAM solution, in addition to providing these capabilities, will be quick to implement, deliver detection capabilities and insights out of the box and require minimal special skills to derive immediate benefits. It should let administrators easily investigate incidents and understand how their privileged accounts are being used.

Section 6

## Assessing the Business Impact of Comprehensive PAM to the Organization

What are the factors that play into the cost and benefit determination, in light of the requirements above? At a high level, three types of factors need to be assessed: financial costs, qualitative benefits and quantitative benefits. Quantitative benefits are relatively easy to determine, based on industry averages and an organization's specific practices. Qualitative benefits are a bit harder to measure, but issues such as time-to-detection, ease of use and the like can have a material impact. The next sections walk you through how to approach each of these.



## Factors in calculating financial costs

Calculating financial costs is generally a straightforward exercise, including the following items:

- Product licensing costs (one-time, subscription)
- Product maintenance costs (second phase and beyond; internal support costs)
- Product deployment costs (professional services, deployment, configuration)
- Training costs (internal customer training, end-user training)

When calculating financial costs, several issues must be considered. First is the cost of a comprehensive solution implementation versus a piecemeal implementation. With a comprehensive solution, the initial cost (including licensing, deployment and training) and any subsequent maintenance will come into play. However, with a piecemeal implementation, the calculation must also include the cost of integration, which can be directly proportional to the number and size of systems to be integrated. If a PAM solution is to be purchased in stages, rather than all at once, there will be incremental procurement, training and deployment costs beyond the basic costs mentioned above. Operating expense (OPEX) costs also factor into a decision to do a piecemeal implementation: additional capabilities often require dedicated hardware, which will need to be budgeted, procured, set up and maintained. The cost calculation should also take into account the resources, time and skills needed if a piecemeal approach is chosen, which presents a real challenge to the budgeting process with so many unknowns.

## Factors in determining qualitative financial benefits

Qualitative financial benefits are sometimes hard to evaluate, but they play a major role when deciding whether to implement a comprehensive solution or do a piecemeal implementation. First, we will consider the piecemeal implementation: Start with a password vault for a few accounts, add more privileged accounts over time, bring in session recording at a later date and, finally, consider user behavior analytics once the entire system is in place.

**Pros:**

- There may be cost savings up front

**Cons:**

- Time-to-value is much longer: it’s impossible to gain visibility fast enough to mitigate risk effectively
- Greatly increased risk in the event of a breach: capabilities such as session recording will require weeks or months of delay for required hardware
- Increases the risk surface for long periods of time
- May require coding or scripting to scale implementation
- Additional cost for hardware, backup and redundancy: longer-term costs will likely be higher
- Vendor lock-in: each time a new module is contemplated, the procurement process starts again; it’s possible that the clock on the previously implemented modules will be reset, meaning a longer commitment to the product than was originally planned

A comprehensive, full-featured and integrated solution that can be implemented in one go, on the other hand, involves selecting a solution with all the needed capabilities at the outset. Although it is possible to turn on the capabilities as needed, everything is ready when you are. This type of implementation—especially when delivered in an appliance form factor—provides mitigation out of the box and requires no special skills to derive immediate benefits. This reduces the workload while avoiding breaches.

Pros:

- Quick to deploy, fast time-to-value
- Immediate protection in the event of a suspected breach: if session recording is needed, it’s a simple matter to turn it on
- Additional capabilities such as analytics are immediately available to ensure control and visibility over the environment
- Greatly reduced attack surface
- Lower total cost: no need for custom coding or scripting, or additional hardware

## Cons:

- Up-front costs may be higher

Certain technological factors can also contribute to the qualitative financial benefits. If the PAM solution leverages user behavior analytics and tight integration with threat intelligence, the ability to detect abnormal activity and take immediate action is significantly strengthened. If multi-site clustering is a feature, this can result in increased availability and faster response time. If the solution is delivered as a virtual or physical appliance, the time to implement will be much shorter than for a software-based solution. Finally, it's important to take into account maintenance costs, which can be considerably lower for an appliance than for a suite of software products that each requires its own dedicated hardware.

The bottom line is that all the above qualitative factors can contribute to lower total cost of ownership, as well as faster time-to-value.

## Factors in determining quantitative financial benefits

When it comes to quantitative financial benefits, take into consideration three key factors: reduction in costs, productivity improvements and revenue protection.

### Reduction in costs

Cost reduction includes avoidance of infrastructure costs, breach-related costs, auditor and compliance fees and unscheduled outage costs. Another factor that cannot be underestimated is the reduction in deployment, maintenance and support costs.

Infrastructure costs can be avoided by choosing an appliance-based comprehensive PAM as opposed to a piecemeal or software-only solution. This is calculated by estimating the number of servers/appliances required for existing or competing PAM solutions, the cost per server, the number of load balancers required and cost for each, and the percent of infrastructure costs that could be avoided with an appliance-based solution.

Breach-related costs include revenue hits, customer notification costs, PR and incident response costs and legal fees. Calculating these costs requires an estimate of the likelihood of a breach (the current estimate is 22 percent over two years) , the volume of records potentially exposed and the cost per record, as well as the cost to remediate and the percentage of these costs that could be avoided with a comprehensive PAM. Since it is estimated that compromised credentials cause more than 80 percent of breaches, this benefit can be significant.

External auditor and compliance costs can be reduced through use of a comprehensive PAM. To calculate the potential reduction, estimate the number of compliance issues per year, the annual cost of noncompliance violations, the external auditor cost to remediate a reportable issue, and the percent of audit finding fees, remediation and compliance penalties that could be avoided through use of a comprehensive PAM.

Another financial benefit comes in the reduced likelihood of unplanned system outages, which can mean disgruntled and nonproductive employees and possibly increased customer churn. This calculation incorporates an estimate of the number of potential business interruptions per year due to breached privileged user accounts, the average downtime per system outage, the cost per minute and the impact of increased availability.

One of the key issues in implementing a PAM solution in a piecemeal fashion is that the cost of maintenance and deployment increases dramatically as each module is purchased, implemented and stabilized. Specific scripting skills are needed, yet how many customers are willing to hire a full-time person to manage, maintain and deploy the solution? Purchasing a comprehensive solution and then implementing capabilities as they are needed avoids this cost.

### Productivity improvements

Enhanced productivity comes in two forms: reduced IT system administrator labor costs and a reduction in implementation and application operating costs.

A comprehensive PAM solution means less system administrator time spent in discovery, policy enforcement, password retrieval or regeneration—and more time available to implement innovative solutions that will move your business forward. To calculate IT system admin labor cost reductions, consider the number of resources and devices with privileged access credentials and the number of accounts per resource/device/app. Then find the number of minutes required for an IT administrator to provide or update privileged access and the average loaded cost per hour, as well as the expected reduction in time to update privileged access credentials through use of comprehensive PAM.

Implementation and operating costs can be significantly reduced through use of an appliance-based comprehensive PAM. To calculate these savings, consider the number of IT system administrators required to implement, host and manage an existing or competing solution and their average loaded cost per hour and per year, and then apply the percent reduction in cost you can expect when choosing an appliance-based comprehensive PAM.

### Revenue protection

A comprehensive PAM can go a long way toward mitigating the most severe financial consequences of a data breach. To calculate this financial benefit, estimate the impact to revenue if your brand were damaged due to a system or data breach and the percent in revenue protection through reduced risk of compromised credentials. A recent Ponemon Institute report shows that for U.S. corporations surveyed in 2016, the financial impact to revenue as a result of diminished brand reputation and goodwill was $3.97 million per year, so PAM can have a major financial impact.

**Section 7:**

## Bringing It All Together

The need for a comprehensive PAM is clear, and the method for calculating the total cost of ownership includes a variety of factors to take into consideration. The costs will depend on whether you choose to implement a comprehensive PAM, enabling features as they are needed, or opt for a piecemeal implementation with full knowledge of the later costs. Keep in mind the costs and benefits of a comprehensive approach:

- Costs are predictable and easy to budget, without additional costs associated with a piecemeal approach (procurement, licensing, training, deployment, resources and additional infrastructure)
- Qualitative benefits are substantial: quick implementation and time-to-value, immediate protection in case of breach, reduced attack surface and lower TCO
- Quantitative benefits are equally impressive: you avoid infrastructure costs, reduce breach-related costs and those associated with audits and compliance, avoid unscheduled outages and reduce the costs of deployment, maintenance and support

The results of these calculations will, of course, vary depending on your situation and organizational preferences, but it is clear that a comprehensive implementation approach results in a much more favorable TCO than does a piecemeal approach to implementing PAM.

**Section 8:**

## Conclusion: A Long-Term View of TCO

Attack surfaces left unprotected grow daily, increasing risk to the organization. A comprehensive PAM solution can reduce the attack surface and provide extremely fast time-to-value, which is what really matters when your organization is in danger of being breached. It provides all the capabilities needed, on day one; while you can initially choose to enable a subset of capabilities, the full power of the solution is instantly available when a suspected breach occurs. By going through the calculations, it is evident that a comprehensive, appliance-based PAM solution makes long-term financial sense, business sense and productivity sense.

To learn more about how CA privileged access management solutions can benefit your organization, visit **ca.com/pam**

**Connect with CA Technologies at ca.com**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

[1] Thomson Reuters, "Cost of Compliance 2016," https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html

[2] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," June 2016, https://securityintelligence.com/media/2016-cost-data-breach-study/

[3] Ibid.