thycotic

PRIVILEGED ACCESS MANAGEMENT

Business Case Playbook

Executive Summary

As our workforce becomes increasingly disparate and fluid, driven by the rise of cloud technologies and mobile devices, identity is emerging as a key concern within information security.

For CISOs and other Information Security professionals, developing a clear Identity and Access Management (IAM) strategy is essential, and within this, Privileged Access Management (PAM) has become a core focus. In fact, Gartner cited PAM as the number one project for CISOs in both 2018[1] and 2019 [2].

"Privileged accounts (or administrative or highly empowered accounts) are attractive targets for attackers. A PAM project will highlight necessary controls to apply to protect these accounts, which should be prioritized via a risk-based approach. PAM projects should cover human and nonhuman system accounts and support a combination of on-premises, cloud and hybrid environments, as well as APIs for automation." (Gartner, 2019 [2])

However, Thycotic research indicates that 66% [3] of CISOs struggle to get the board to understand the business case behind any form of cyber security.

This Playbook brings together the key information and statistics that are needed to support a successful business case submission for a PAM project. However, this does not limit its application to business leaders. The playbook can also be used as an introduction to PAM for anyone who wants to understand what is driving the adoption of these tools in their industry.

What makes a great business case?

Most IT or security projects require a formal approval process, and that often includes a written business case. These documents can vary from a simple one-page write-up to a full-blown justification paper with detailed cost and return-on-investment (ROI) calculations. Your proposal for a PAM solution is likely to need the following information:

Statement of the problem

Detail the issues/challenges that PAM will help you solve

Analysis of impact

Explain the impact on the business of solving the problem. For PAM this means covering:

Security Risks and Threats

What are the key threat vectors and cybercriminal behaviours at play – for example, external threats and impersonation, third parties, internal threats, non-human vectors, excessive endpoint privileges? What risk does this pose? How does PAM help mitigate these?

Compliance and Audit Issues

Which compliance and audit requirements affect your business, and which require controls and intelligence for Privileged Access? How can PAM help you get the visibility and control you need to ensure you can meet any compliance?

Operational Issues and Pains

What are the key areas of operational pain that a PAM solution will help resolve and where will it add value: for example, forgotten passwords, requirement for help desk staff, manual password rotation, discovery and inventories, JML processes and creating in-house solutions.

Options and other possible solutions

Set out how you explored the market and/or solutions for this issue with pros and cons of each option. Consider things like, is it possible to deliver a fit-for-purpose solution with existing solutions of an in-house development? Explain why PAM is more suitable than other popular solutions such as IAM or password management?

Recommended solution/Total cost of ownership (TCO)/Return on investment (ROI)

Explain what you are recommending and why, including hard costs, soft costs, total cost of ownership, return-on-investment calculations, and how this aligns to corporate or IT department strategy.

Project proposal

Illustrate how you will implement the solution, including timing, technology needs, staff needs, risks and whether they can be mitigated.

This document will guide you through all of these stages in detail so you can confidently understand the business case for PAM in general.

SECTION 1: The problem

The beginning of the business case should detail the business risks and challenges that privileged access management will help you solve.

In most cases, this section can only be accurately written once the full scope of the business case has been mapped out in the subsequent sections. Each business will need to evaluate the weight of the different kinds of business risks and the corresponding business benefits that privileged access management will bring to them. With this in mind we can begin to review the analysis of impact.

SECTION 2: Analysis of impact

As we mentioned above, implementing a PAM solution will impact your business in three key ways:

Mitigating security threats

Managing challenges with compliance

Solving a range of operational issues and pains.

1 | Security Threats

Network breaches over the past decade have demonstrated that privileged accounts are vulnerabilities that pose a serious threat to organisations. Research and statistics across the board continue to focus on privileged accounts as a key security risk.

Forrester estimates that 80% [4] of security breaches involve privileged credentials. Elsewhere, according to Verizon, 66% [5] of successful breaches leverage privileged accounts, with 89% of privilege misuse incidents caused by internal actors. On top of this, nearly one third (32%) of respondents to Thycotic's Black Hat Survey [6] said accessing privileged accounts was the number one choice for the easiest and fastest way to get at sensitive data.

What are Privileged Accounts and why are they such a target?

Privileged Accounts are credentials that offer users access to administrative functions and other privileges that offer powers above and beyond those normally given to business users. Examples include active directory accounts such as domain Administrators or database root accounts that have vast power. In the hands of cyber criminals and malicious insiders, these accounts can grant them the capabilities and scope to execute their plans, allowing them to impersonate standard administrators, change critical security and operational settings, identify means to further elevate their privileges, and potentially cover their tracks in the process.

Increasingly the attack surface extends to include privileged accounts in the cloud (such as IaaS/PaaS environments and SaaS applications), endpoint privileges (administrative powers granting privileges on clients and servers), exposed credentials in DevOps workflows, service & application accounts, the Internet of Things, Operational Technology, and even Robot Process Automation workflows.

Ultimately the definition of what constitutes a privileged account is really up to the business itself and its own evaluation of what accounts, systems, and users, require advanced protection from malicious action.

Privileged Users

It's also important to remember that threats don't always come from outside.

If you're implementing a PAM solution there are a number of areas you need to be aware of when defending against privilege misuse, these include:

Internal Privileged Users

As your privileged user base grows it becomes much harder to track usage of privileged accounts. In a large business it is also difficult to determine motives, instill company loyalty and bring staff in line with a single vision. All of these challenges make it unrealistic to rule out insider threats (malicious or accidental) in the enterprise.

A story from Tesla [7] in June 2018 highlights the damage that is possible from the inside. The company announced it had successfully sued a former employee after they had made direct code changes to the Tesla Manufacturing Operating System under false usernames, potentially damaging several aspects of the businss operations simply by having too much access and privilege.

When an enterprise has critical business operations that can be harmed by disgruntled employees there needs to be extra security applied to address this risk.

Third Parties

Sometimes third parties, such as partners or consultants, need to access privileged accounts in order to perform their work. These entities provide an amorphous attack vector that can be hard to measure and control. The Target breach in 2013 [8] is a great example of what can go wrong if third parties are not properly managed: In this case, cyber attackers used stolen credentials from a third-party vendor to hack into Target's gateway server and access a customer-service database, where they installed malware to cull customer data, including credit-card information and contact details. The cost of the breach is now estimated to have cost Target over $300 million.

External Actors

As mentioned above, cyber criminals see Privileged Account access as a strategic objective in order to achieve their goals with a third of malicious operators seeing it as the primary objective, according to Thycotic's Black Hat Survey [6]. The relentless phishing and spear phishing attacks that an enterprise experiences are motivated by a desire to gain credentials, and then to move laterally through a network in order to elevate privileges.

Increasingly attackers are opting for a low and slow approach too – meaning they use this privileged access over a long period to slowly gather information and plan a more calculated attack.

Internal Business Users

Business Users have access to credentials and intelligence that can be used to access privileged accounts. An employee with local admin privileges, an employee with non-IT administrative privileges (social media, HR systems, or financial systems for example) or even an ordinary employee's Active Directory credentials all have value to begin lateral movement through the business.

Non-Human Users

More and more, privileges are used and stored by non-human elements. Service accounts, hard coded credentials, DevOps workflows, application-to-application authentication, APIs and process automations are all problem areas for businesses trying to guard their privileged credentials. Management of non-human privileged access is often left under-protected as traditional password vaulting and IAM capabilities fail to provide meaningful governance and management capabilities without compromising critical operational pace.

Some recommended additional reading:

Anatomy of a Privileged Account Hack

https://thycotic.com/resources/anatomy-of-a-privileged-account-hack/

Thycotic's Black Hat Report

https://thycotic.com/resources/black-hat-2019-hacker-survey-report/

2 | Compliance and Audit

With the growing focus on compliance, many regulations are spelling out the requirement to manage privileged access. Not doing so can result in audit failure, compliance shortfall and fines. GDPR, HIPPA, ISO 27001, SOX, PCI-DSS, NERC, NIST, and many others, all require security controls, auditing, and monitoring, in the area of privileged access (you can find more on this in our Global State of Compliance [9]).

Throughout global compliance mandates there are repeated requirements that fit into key themes. These are broken down in detail in Thycotic's CISO's Quick Guide to Access Control Compliance . Making progress on these 5 key areas will enable businesses to advance their compliance to key global standards.

5 key areas:

- **# 1** Having a well-defined privileged access control policy
- **# 2** Secure and controlled access to privileged accounts, systems and applications
- **# 3** Reinforced privileged access with multi-factor authentication
- **# 4** Discovery of privileged accounts to enforce password reset and management
- **# 5** Audit and monitoring of privileged account usage

The cost of failure

For businesses subject to compliance, failure to attain key access control mandates has potentially much larger repercussions:

Failure to meet compliance can lead to fines

Failure to comply to GDPR can lead to fines of up to 4% of annual revenue[10], with the International Commissioners Office implementing fines as high as £180 million[11] in 2019.

Impact on Operations

Some failures have significant business impacts in terms of partnerships and operations. For some, failing to meet key standards can mean losing critical customers and therefore slowing business growth.

Reputation damage at multiple levels

Headline inducing fines, failure to attain compliance, severance of relations and partnerships on the basis of compliance failure and the impact of sensationalist journalism, have consequences that are not easy to quantify.

Lost business relationships opportunity

Lastly, failed audits or public fines can cause some issues in business relationships. In some cases, this is because a business may require their supply chain partner (for example) to be ISO 27001 certified in order to continue their relationship. Or, in other cases, it may just be more informal. Consequently, a business that risks privilege abuse or compliance failure also risks additional business opportunity.

To mitigate these risks businesses must aim to meet compliance mandates but doing so can be a major drain on resources, especially for businesses that face many overlapping requirements that re-articulate the same themes in different terms.

3 | Operational Cost

It is often overlooked just how many hours are lost due to the absence of proper Privileged Access Management. Poor management of privileged access can lead to significant operational damage. If a privileged user leaves, or even just forget their credentials, there is a loss of productivity. In the best-case scenario, the help desk can authorise new credentials, in the worst-case scenario a critical system remains inaccessible, causing damage and lost opportunity.

On top of this, in the modern enterprises a typical privileged user may need to remember credentials for a large number of accounts. This results in cyber fatigue, forgotten credentials, weak credentials, credentials being stored in unsafe systems such as an excel sheets, or, worst of all, all accounts using the same credentials.

Here are some of key operational business risks that form part of the PAM business case:

Help Desk Time

Managing passwords not only affects the speed and effectiveness of IT admins, but also the help desk which is burdened with ongoing requirements for password resets and other creative work arounds.

Failed Provisioning

Without a proper PAM solution in place to deliver Role Based Access Control (RBAC), the business may resort to miss-allocating the appropriate privileges users require. PAM enables businesses to quickly and effectively provision access to the systems a user or a team require. Users who don't have the correct access rights will be more of a drain on support resources because they will bother the service desk unnecessarily and be less productive as they wait for IT to respond.

Removal of Local Admin Privileges

One of the most prevalent and challenging privileged accounts are Local Accounts with administrative privileges on endpoints.

Commonly known as local administrators, this is a user account that can manage a local computer. Generally, a local administrator can do anything to the local computer but is not able to modify information in Active Directory for other computers and other users.

IT security often cannot tolerate the sheer amount of privilege this gives to end users and the risk this poses if their endpoint is compromised.

Consequently, Local Admin rights are removed, but this means that end users are unable to perform certain functions or run certain applications that are required in order to perform their jobs. This means lost productivity and, in the case of developers, often lost talent and higher turnover of employees.

Accidental damages

If employees have privileges that exceed the scope of what their job requires, this can lead to accidental damages. There is a direct relationship between the privileges an individual has and the possibility of operational damage.

What needs to be done in order to address these pain points

In summary, there are three key areas of business risk:

Data Breach through Privilege Abuse resulting in financial, reputational and operational damages

Compliance and Audit failure resulting in fines and lost business relationships

Operational Damage resulting in lost opportunities, slower innovation and less business output

This is a rough sketch of the steps businesses need to take to address these concerns, all of which can be implemented within a fully functioned PAM solution:

1. Discover and establish visibility of privileges and privileged accounts.
2. Once visible, privileged access should be granted under a principle of Least Privilege that ensures users and systems only have access to other accounts and systems, applications, and commands that they need in order to do their job.
3. Due to the vast possibilities of how to assign privileges to users, this key element of administration should be intuitive and able to be done from a single pane of glass.
4. All privileged activity should be recorded, tracked and reported on for retrospective auditing/forensics. This should include not only which accounts and systems were accessed, but also, session video and metadata so the actual activity can be searched and reviewed.
5. All privilege activity should be directly tied to the privilege user to ensure direct accountability.
6. It should be possible to immediately revoke privileged access from human and non-human usage once it is no longer needed.
7. There must be controls put in place to rotate privileged credentials as often as possible
8. Users should have access to the accounts and systems they need without having to remember or see passwords.
9. Strong authentication should be in place for all privileged access. This should deliver a zero-trust model that measures users based on multi-factor authentication, single sign on, user analytics and other intelligence.
10. Privilege Account usage should be subject to live intelligence and alerting to identify privilege miss-use pro-actively. The ability to integrate with existing intelligence tools.

These capabilities should extend across the privileged attack surface to include the environments relevant to the specific business requirements. For example, businesses that need to grant business users admin rights on their endpoints and require credentials in DevOps workflows will need to ensure that these principles extend to these environments, ideally from a single pane of glass.

A business with these capabilities across their privileged environments will make significant progress across all 3 key challenges of security, compliance, and operations.

4 | What are the options and alternatives

So, what are the alternatives to PAM? It is possible to provide some internal solutions that can address some concerns. For example, it's possible to use a combination of spreadsheets and password management tool to centralise the management of privileged credentials and potentially attempt to track usage. However, these internal methods can often raise a number of unacceptable challenges.

There are a number of needs that these solutions often fail handle, all of which are critical to securing your business in line with the challenges set out in Section 4:

1. **Discovery**
   While some tools can help you start identifying privileged accounts, they will lack the breadth, precision and simplicity to successfully identify privileged accounts and to view them from a single pane of glass. Without ongoing identification and onboarding of new privileged accounts a solution loses its efficacy in managing privileged access.

2. **Password Rotation**
   Credential rotation is likely to remain a manual job, especially for things like Service Accounts. Even if you attempt to use automated scripting it is still hard work and assumes you already have clear visibility of ALL your privileged accounts.

3. **Protecting all privileges, not just user passwords**
   If you're a growing, evolving organization with diverse technology and a dispersed workforce, a technology like a password management system won't be able to keep pace with your requirements.

4. **Syncronisation**
   Wherever you are keeping your privileged credentials, you need to be sure that they are valid and that they have not somehow been edited at source, leading to a security issue and the failure of your PAM solution. For a business that is managing hundreds, thousands or tens of thousands of credentials a manual process for this is unacceptable.

5. **Multifactor Authentication**
   With MFA increasingly required as standard in compliance mandates it is essential to ensure privileged access requires some form of MFA. This raises a serious challenge; how does a business successfully apply MFA to so many different types of accounts and systems? This requires vast amounts of customisation and support. As well as this there is increasing appetite for adaptive and intelligent M2FA challenges based on threat levels.

6. **Monitoring and Reporting for Compliance**
   Securing passwords that provide access is not enough to satisfy auditors that you are keeping privileged accounts safe. You need to know what users did while accessing those privileged accounts.

7. **Continual development and innovation**
   Even if a business can build a PAM solution that is acceptable, how can it maintain its suitability to the businesses changing needs and the evolving threat landscape?

This is by no means an exhaustive list, however, it starts to highlight the need to purpose built and innovative solutions. These challenges are further exacerbated as an organisations privileged attack surface expands to include complex requirements such as DevOps workflows or service account governance.

5 | TCO and ROI

Writing a business case for an IT project, including a PAM solution, can be a rewarding project where you uncover significant benefit to your organisation beyond the obvious monetary gains or savings. But it can also be a challenge to quantify that. As such, one of the most difficult parts of building a business case is calculating return on investment (ROI) and total cost of ownership (TCO).

The simplest formula for return on investment is:

(Savings + income) / costs

While it looks like an easy formula, determining how you calculate the savings, income and costs can be daunting. You need to take a number of things into consideration when making these calculations:

- Effect on revenue
- Effect on costs
- Effect on productivity (IT and corporate-wide)
- Effect on product or service delivery (faster time to market or new competitive advantage)
- Risk of non-compliance (internal and external)
- Risk of breach or hack (internal and external)
- Value of IT maturity

For TCO, you should consider not only software and support costs, but also the cost of infrastructure, professional services, supporting technology, and internal operations to support the project.

Specific ROI for PAM projects

Here are the key points you can use to quantify the impact of adopting a PAM solution:

Reducing the risk (and cost) of a security breach

According to the 2019 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute report [12], the global average cost of a data breach is $3.92 million, up from $3.86 million in 2018. A key finding is that the average total cost of a data breach is 95% higher in organisations without security automation deployed; security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. A key part of security automation is PAM, and Gartner estimates that by 2021, organisations with PAM will have a 50% lower risk of being impacted by advanced threats [13]. Other related costs are: termination of business partnerships, bad publicity for your organisation, lawsuits from entities whose data was compromised and loss of trust and revenue from your customers.

Average total cost of a data breach is **95% higher** in organisations **without** security automation deployed

Process automation to reduce labor costs
This calculation can be based on the time that your IT admins spend on tasks that will be automated by the new PAM solution and calculated based on the cost of FTEs (full-time equivalents). Labour costs can be anything from calls to the help desk for help with privileged accounts, to discovering, managing and rotating passwords, to providing detailed reports and audit information to internal and external audiences.

The global average cost of a data breach is **$3.92 million**

Avoiding non-compliance fines and costs
Depending on the industry and compliance regulation, fines can vary greatly. You should understand each regulation and the associated fines you can expect for non-compliance, as well as how your PAM solution mitigates risk related to non-compliance.

6 | Project Proposal

Once you've set out why you need a PAM solution and the real benefits/savings it's going to bring to the business, you need to set how you're going to implement the solution, including timing, technology needs, staff needs and the potential risks.

Accurately resourcing and predicting implementation and maintenance costs can be a tough call. These are costs that are often under-represented in many business cases as all vendors sell their solutions as suitable for deployment. So, in order to properly determine complexity of deployment and possible spiraling costs businesses must find a way to measure this.

Below we'll set out one way to measure of your project complexity effectively, by breaking it into three areas, customisation requirements, architectural requirements and employment and skill requirements, and providing a checklist of issues to consider.

Customisation Requirements

In order to properly evaluate this, you need to consider the following:

- What are the accounts, systems and apps you need to launch/connect to from PAM solution?
- How many and what percentage of these require custom work from the vendor?
- Has your vendor taken this into account in the PS (price cope) and time frames?

Warning: Customisation requirements can render acquired PAM licenses useless until previously undiscussed fees are paid in order to adapt the tool to meet the requirements. So make sure you ask about the need to create custom launchers, integrators, password rotators, reports, discovery scanners and anything else you need to make the solution work for your business.

Architectural Requirements

Again, there will be specific requirements for your company's network architecture that will impact on the cost of roll out, so ask yourself these questions:

- What environments, logical and geographical does your deployment need to reach/support?
- What vendor architecture is required in order to deliver this?
- What professional services and maintenance is required in order to successfully deploy this?

Warning: Larger and more complex architectures will inevitably take longer to deploy. As well as this, bare in mind if the nodes are proprietary software and whether they require vendor consultancy to perform key functions such as upgrades and installation.

Employment and Skill Requirements

Staffing can be one of the hardest areas to predict and cost but answering the following will help you manage expectations effectively.

- How many full-time employees is your vendor suggesting you will need?
- How much training and knowledge transfer needs to take place in order to enable successful running?
- Does training cost money?
- How difficult do your staff find the software?
- Is it possible they may abandon attempts to use it?

Warning: Unintuitive and clunky administrative experiences can, at best, leave your project over-budget, or at worse, lead to a limited or failed deployment. Make sure to rigorously test the admin console and the standard experience required in order deploy. Avoid test environments built by the vendor. We strongly recommended that to measure these concerns you plan to run a full proof of concept trial with any solution.

Recommended additional reading:

Is Your Software Simple?
Assess How Well the PAM Software You Choose Supports Your Goals

This whitepaper provides a checklist of questions to ask your vendor before taking the plunge.

https://thycotic.com/solutions/free-it-tools/pam-software-vendor-checklist/

4 | Summary and Recommendations

With so many business benefits as well as security and compliance risks business leaders can use the information in the playbook to deliver a compelling business case that achieves the following results:

- Brings attack vectors and cyber-criminal behavior to the business's attention
- Highlights the increasingly regulated environment and how compliance mandates require action in access control
- Gives a fair review of in-house proposals and highlights their limitations
- Demonstrates the value of purpose-built solutions like Secret Server in this context

ABOUT THYCOTIC

The easiest to manage and most readily adopted privilege management solutions are powered by Thycotic. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, D.C., Thycotic operates worldwide with offices in the UK and Australia.

www.thycotic.com

Sources

1. Smarter With Gartner 2018
   https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/
2. Smarter With Gartner 2019
   https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/
3. Thycotic
   https://thycotic.com/resources/cyber-security-executives-survey-report-europe/
4. Forrester Wave™: Privileged Identity Management, Q4 2018
   https://www.forrester.com/report/The+Forrester+Wave+Privileged+Identity+Management+Q4+2018/-/E-RES141474
5. Verizon 2017 Data Breach Intelligence Report
   https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
6. 2017 Black Hat Hacker Survey: Fastest, Easiest Ways To Get At Your Critical Data?
   https://thycotic.com/resources/black-hat-2017-survey/
7. Tesla saboteur trains spotlight on insider threats
   https://www.scmagazine.com/tesla-saboteur-trains-spotlight-on-insider-threats/article/774976/
8. Target to pay $18.5M for 2013 data breach that affected 41 million consumers
   https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/
9. 2018 Global State of Privileged Access Management Risk & Compliance
   https://thycotic.com/resources/2018-global-state-of-pam-compliance/
10. What are the GDPR Fines?
    https://gdpr.eu/fines/
11. BA faces £183m fine over passenger data breach
    https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways
12. Cost of a Data Breach Study (IBM/Ponemon)
    https://databreachcalculator.mybluemix.net
13. Gatner Best Practices for Privileged Access Management (September 2017)
    https://www.gartner.com/en/documents/3800163/best-practices-for-privileged-access-management