PRIVILEGED ACCESS MANAGEMENT

TOOLKIT

SILA | silasg.com

TABLE OF CONTENTS

ALL OF THE PAM TOOLS YOU NEED TO BUILD A PROGRAM IN ONE UNIFIED KIT

Welcome to Sila's Privileged Access Management (PAM) Toolkit! Our PAM practice specializes in helping complex organizations define, implement, and maintain privileged access solutions and we're excited to share our experts' insights as well as some of our tips and tricks. This toolkit contains a blend of articles and worksheets to help you define actionable steps toward an effective PAM program that aligns with your organization's business goals to deliver maximum value. From planning to implementation to governance, we hope this toolkit helps you strengthen your organization with PAM solutions that set you up for long-term success.

GLOSSARY

ABOUT THE AUTHORS

CATHY HALL

Cathy is the Privileged Access Management (PAM) Practice Lead at Sila. She has nearly 20 years of experience providing IT services to Fortune 500 companies and government agencies, specializing in PAM, Identity and Access Management, Information Security, and Enterprise Applications. Cathy brings a unique mix of Federal and Commercial cybersecurity experience and uses her deep knowledge of NIST and other industry frameworks to drive security architectures. She is an active cybersecurity writer, speaker, and mentor.

TAPAN SHAH

Tapan is a Managing Director at Sila and heads the National Consulting Practice. He brings over 25 years of experience and industry eminence in cybersecurity and risk, with contributions to multiple publications, conferences, and advisory boards. His career has been dedicated to working with senior executives of Fortune 500 companies, helping them apply governance, process, and technology to improve their cybersecurity and risk posture.

CATHY AND TAPAN WOULD LIKE TO THANK THE SILA PAM TEAM FOR THEIR SIGNIFICANT CONTRIBUTIONS TO THE CONTENT IN THIS TOOLKIT.

INTRODUCTION

MAKE YOUR PRIVILEGED ACCESS MANAGEMENT PROGRAM A MISSION, NOT A MANDATE

Privileged Access Management (PAM) protects the keys to the kingdom – access to the privileged administrative accounts that control your organization's critical servers, databases, and networks.

A hacker, malicious insider, or negligent user who can access these administrative accounts can go on to compromise or corrupt anything from customer data to financial systems. A strong PAM program helps prevent, detect, and mitigate such abuse of privileged access and works in concert with other security and identity and access management (IAM) systems at your organization. The goals of a PAM program should include:

- □ **Protecting your critical data and ensuring the availability of essential business systems**
- □ **Reducing the likelihood that administrator credentials will be compromised or misused**
- □ **Reducing the impact if compromise or misuse does occur**
- □ **Pinpointing which user is responsible for actions taken by a shared account**

Your organization may be ready to begin building a long-term, broad-based PAM program from the start; however, your organization may begin considering a PAM program to meet an immediate, urgent need. For example, it might be a CISO looking to ensure passwords for SOX-relevant systems are accessed through a secure vault or to respond to an audit finding on security processes around specific sensitive assets.

But just satisfying a mandate to protect a limited number of accounts or applications is a narrow goal: it doesn't make the most of your PAM investment and could make your organization less secure overall. The point where you've satisfied your PAM mandate shouldn't be the end of the road, but the beginning of a mission to protect all of your critical privileged access. This mission-based approach delivers the highest return on investment (ROI) by making an increasing number of your accounts and systems more secure over time.

This article is the first in a four-article series from Sila on building a strong PAM program via a mission-based approach. Over the course of the series, we'll introduce you to key differentiators between mission and mandate approaches to PAM and their outcomes, how to determine if you're ready for mission-based PAM, critical steps to deploying PAM securely, and applying robust governance for long-term PAM success.

THE NEED FOR PAM

PAM is becoming more important by the day. The attack surface of applications and platforms through which hackers can compromise administrative accounts is expanding, the sophistication of attackers is growing, and the risks of successful attacks, including regulatory fines and brand reputation damage, are mounting.

And these concerns are only going to continue to increase. In a January 2019 report, market researcher Gartner estimated that:

> **BY 2022, 70% OF ORGANIZATIONS WILL IMPLEMENT (PAM) PRACTICES FOR ALL USE CASES IN THE ENTERPRISE, WHICH IS A SIGNIFICANT INCREASE FROM 40% TODAY.**

Gartner also predicted that "by 2022, 90% of organizations will recognize that mitigation of PAM risk is a fundamental security control, which is an increase from 70% today." [1]

Your organization probably has a method to protect privileged accounts. But it might rely on manual, less secure methods to track access to accounts and manage credentials. You may also have different PAM methodologies of varying quality and effectiveness across your business units and locations. This not only increases the chance of inconsistencies that can be exploited and manual errors but makes it significantly harder to identify and mitigate risks.

[1] Gartner, Inc., Best Practices for Privileged Access Management Through the Four Pillars of PAM. January 2019.

PAM AS A MANDATE

A successful attack or stern note from an auditor or regulator can provide a valuable kickstart because it identifies a real problem and begins to educate business stakeholders to the importance of PAM. However, not moving beyond such a mandate approach has real limitations, especially if it:

☐ **Solves the vulnerabilities an auditor or regulator cares about but not those which may be most critical to your business**

☐ **Makes routine administrative access so difficult that users seek to find ways around your PAM system via means you cannot track or manage**

☐ **Fails to remove non-authorized methods to get to privileged access that has been vaulted**

☐ **Provides a false sense of security based on a small number of protected accounts and systems, with no plan to identify and protect other assets that are or may become important to your business**

☐ **Views PAM as a standalone system rather than an integrated part of your organization's overall security, IAM, and analytics ecosystem**

For all these reasons, staying too long with a mandate approach can limit the number and importance of risks PAM can reduce as well as user adoption. Getting the greatest benefit from your PAM program investment requires a broader vision.

PAM AS A MISSION

Here are four points on how embracing PAM as a mission improves upon a mandate approach.

Identifies the biggest risks to your business

A proper PAM implementation begins with an in-depth assessment of which systems and accounts are most critical to your business, how you are managing them, and which risks require the most urgent attention. This includes asking for, and listening to, different definitions of privileged access from different stakeholders.

Encourages user adoption

A mission approach requires building partnerships with your administrators. Acknowledge that PAM will introduce changes to how your administrators carry out their daily tasks, design the solution so it is as easy to use as possible, and explain why PAM is good for the business and the users in the long run.

Protects the right accounts and platforms
A dedicated PAM management and governance team can assess which new accounts and platforms to protect over time, and how. It also makes sure you're doing enough and the right kind of training, and that you are integrating your PAM platform with other security functions to give you the most timely and proactive view of your risks.

Examines broader technical issues that can leave you vulnerable
Proper design of your PAM infrastructure helps ensure its availability and resiliency, which is essential because (if done right) PAM will become mission-critical. Hardening the PAM solution and its infrastructure can also identify other security needs, such as multifactor authentication on your password vault or unnecessary open ports on your servers.

BOTTOM LINE BENEFITS

A mission-based approach to PAM is worth the investment and delivers far more to your organization than a mandate approach can, including higher overall ROI and benefits over a longer period of time through a more comprehensive and risk-based security approach.

Mission-based PAM helps organizations be more secure and compliant through detailed, automated account usage tracking and mitigates threats more quickly and accurately through data sharing across security platforms. Finally, it helps to foster increased user adoption and acceptance as part of the organization's security culture, a powerful benefit which shouldn't be underestimated.

ARE YOU READY FOR MISSION-BASED PAM?

In our first article, we explained how privileged access management (PAM) ensures that only authorized administrators can control your vital systems. We also described the journey organizations often take to implement PAM tools and processes.

Organizations often begin their PAM journeys with a mandate, for example responding to a specific audit finding or regulatory requirement, such as a failure to properly rotate credentials or lock down passwords in a secure digital vault. Ideally, over time they migrate to a “mission” approach which has a broader goal of strengthening and modernizing the organization’s overall security strategy and aligning with industry best practices. In Sila’s experience, staying the course with a mandate approach delivers less value over time because it is designed to meet only a limited set of security requirements. It may increase your risk by forcing users to work around the PAM solution to do their jobs efficiently.

Following a mission-based approach, whether from the start or shifting towards one over time, makes the most of your PAM investment by protecting more of your systems, maximizing user adoption, and sharing data among security systems for a deeper, contextual understanding of risk and how to manage it.

The following are five questions that will help determine whether your organization is ready to move towards a mission-focused approach to PAM.

1. DO YOU HAVE THE BACKING FOR A MISSION-DRIVEN APPROACH?

Mandates can be relatively easy to get support and funding for because they often have a powerful sponsor, such as an auditor, regulator, or chief information security officer (CISO). Mandates can also be easier to adopt: business units may see compliance as a one-time exercise and believe they can then get on with carrying out their “real” work using the same tools and methods as before.

Mission-driven PAM takes a broader, long-term view towards improving organizational security; it may take more funding and effort to initially build, but the multi-year return on investment is better. Helping your organization to understand that the long-term benefits of a mission-driven approach are worth the additional initial investment requires sponsorship from senior executives and other key stakeholders.

You can build the case for a PAM mission by describing how much the organization is spending to "check the box" to meet a mandate, and how a PAM mission can deliver far more visibility into user sessions and enable it to stop suspicious activities. You can also explain how a limited PAM program can increase risk by forcing users into unmonitored access you cannot track, much less stop, providing a prime target for malicious actors seeking to control sensitive assets.

2. HAVE YOU DEFINED WHAT PRIVILEGED ACCESS MEANS TO YOU?

If not, you won't be able to focus your time, money, and effort on the most critical areas. Accurately defining privileged access requires identifying and forging a relationship with everyone who has a stake in the program, such as the CISO, infrastructure team, managers of your security operations center, and managers of identity and access management (IAM) programs.

Have you educated them on your definition of privilege and asked them for theirs? Have you asked for their feedback on your PAM implementation plan? Doing so will increase their cooperation and provide valuable insights into what you need to protect, how to protect it, and how to share data with other systems and processes to maximize your security and return on investment.

3. ARE YOU WILLING AND ABLE TO TREAT YOUR ADMINS LIKE PARTNERS?

> "CREATING TRUSTED PARTNERSHIPS AT ALL LEVELS IS A CRITICAL PART OF ENSURING A SUCCESSFUL PAM JOURNEY"

Work closely with your administrators as well as your managers and senior leaders. Listen first to understand their current processes and pain points and then show them the improved security and lower stress that PAM processes can provide not only for the organization at large but for their particular areas of concern.

4. ARE YOU WILLING TO MAKE THE PARTNERSHIP REAL BY DOING THE HARD WORK OF ORGANIZATIONAL CHANGE?

In the short run, PAM will require changes to how administrators do their jobs. Invest time and resources to minimize disruptions, rather than forcing them to use the new system as quickly as possible without taking change management steps to ensure a positive, efficient user experience.

For example, a Unix administrator might leverage an insecure, but easy-to-use, saved SSH session to log into a server. A typical initial PAM rollout in response to a mandate might force the admin to go to a website and enter a second password to get the actual Unix administrative password. A more user-friendly implementation might include a proxy server that lets the admin use their favorite SSH tool and a second password but eliminate the need to go through the Web site. Seeing your admins as partners and taking the time to understand their existing processes (and shortcuts) lets the PAM team understand what more efficient options and features they should consider prioritizing as you roll out your PAM system.

5. DO YOU HAVE A PLAN TO CONTINUALLY ONBOARD NEW PLATFORMS AND PROCESSES AS YOUR BUSINESS NEEDS CHANGE?

You need to create a team whose job is to monitor, manage, and expand your PAM implementation over time. Without such ongoing oversight, your PAM solution only represents a point in time and will become increasingly stale and ineffective as new privileged accounts are created outside of the controlled PAM process. Focusing exclusively on vaulting or securing today’s privileged access can cause you to lose sight of your needs as your business grows and changes.

Begin your planning by understanding which systems are most critical to you. For a financial institution, it might be a trading system where downtime or a breach could cost hundreds of millions of dollars. For a pharmaceutical company, it might be the platforms that store the latest research compounds or patient trials. For a social media company, it might be the systems that store user profile data. Realize every owner will say their system is most important, but don’t let them spend too much time debating. Get a good feel for which systems and accounts are most critical and validate those priorities with more senior managers. You’ll also want to avoid a heavy PAM investment in a platform that’s due for upgrade or replacement.

PAM ✓ CHECKLIST

WANT TO TAKE YOUR PAM PROGRAM TO THE NEXT LEVEL?

Many organizations begin their Privileged Access Management (PAM) journey to meet a mandate, such as an audit finding. Mandates can highlight critical needs but are limited in nature and don't often encourage organizations to build solutions focused on advancing the mission of their business. Adopting a mission-based approach to PAM aligns security with business goals to deliver enterprise-wide, long-term value. Find out if you're ready to take your PAM program to the next level through a mission-based approach with the following questions.

QUESTION 1: DO YOU HAVE THE BACKING FOR A MISSION-DRIVEN APPROACH?

□ Evaluate the organizational risks associated with your current state and the benefits of reducing those risks with a more holistic, mission-driven approach to PAM

□ Identify a strong sponsor to champion your PAM program and advocate for its needs and value

□ Help stakeholders at all organizational levels understand the value of mission-driven PAM in relation to their own needs and priorities

KNOW THE FACTS

PRIVILEGED ACCOUNT ACCESS MISUSE IS THE SECOND MOST PREVALENT CAUSE OF CYBERSECURITY BREACHES AND INCIDENTS

2018 DATA BREACH INVESTIGATIONS REPORT | VERIZON

QUESTION 2: HAVE YOU DEFINED WHAT PRIVILEGED ACCESS MEANS TO YOU?

- □ Work with stakeholders across your organization to build a definition of what "privilege" means and what access it pertains to

- □ Use your definition to identify and map your organization's privileged access, including in the cloud

- □ Prioritize areas for PAM integration in consultation with your stakeholders

QUESTION 3: ARE YOU WILLING TO TREAT YOUR ADMINISTRATORS LIKE PARTNERS?

- □ Create and sustain trusted partnerships with stakeholders at all levels

- □ Work closely with your administrators to understand their current processes and pain points

- □ Ensure your plans and priorities incorporate your administrators' input and show them how the PAM solution will address their needs, as well as those of the broader organization, over time

QUESTION 4: ARE YOU WILLING TO MAKE YOUR PARTNERSHIPS REAL BY DOING THE HARD WORK OF ORGANIZATIONAL CHANGE MANAGEMENT?

□ Invest time and resources to help administrators adjust to the new PAM tools and processes

□ Seek to minimize disruption to administrators over implementing changes as quickly as possible

□ Educate and communicate with stakeholders at all levels in ways appropriate to their involvement to encourage a positive user experience and successful adoption

KNOW THE FACTS

THE GLOBAL AVERAGE COST OF A DATA BREACH IN 2018 WAS $3.86 MILLION

2018 COST OF A DATA BREACH STUDY | PONEMON INSTITUTE

QUESTION 5: DO YOU HAVE A PLAN TO CONTINUALLY ONBOARD NEW PLATFORMS AND PROCESSES AS YOUR BUSINESS NEEDS CHANGE?

□ Communicate the perspective that PAM is an ongoing activity and investment

□ Create or designate a team to be responsible for ongoing PAM management and expansion to ensure new systems and their privileged accounts are incorporated into your PAM solution over time

□ Track your organization's growth and change to understand how your PAM program may need to adjust to continue to align with business priorities

KNOW THE FACTS

56% OF RESPONDENTS SAID INFORMATION LOSS OR THEFT WAS THE TOP FACTOR IN JUSTIFYING CYBERSECURITY SPEND

2019 CYBER RESILIENT ORGANIZATION STUDY | PONEMON INSTITUTE

FIVE STEPS TOWARD A SUCCESSFUL PAM IMPLEMENTATION

You know the best way to handle privileged access management (PAM) isn't to simply check a box to satisfy a mandate, it's to view it as a mission. A mission-based approach ensures you improve security across your whole enterprise over time, rather than only satisfying a limited, one-time mandate.

However, you may be wondering where to begin and what it will take to build your PAM mission. Here are five focus areas we've found essential to providing the most protection for your administrative accounts, the best data to help you assess and remediate risk, and the fastest adoption by users.

STEP 1: ASSESS YOUR CURRENT STATE

You can't improve your PAM implementation if you don't know where you're starting from. That requires understanding your current business processes and priorities, how administrators currently access your privileged accounts, and which PAM deficiencies pose the greatest risk.

Pay particular attention to local administrative accounts, which combine high levels of privilege with little or no oversight. They expose you to significant risk and thus are a top priority for your PAM program. You'll need to understand who uses such accounts and how you can bring them under the control of your PAM tool (more below).

Understanding your current PAM processes and tools will benefit from building strong relationships with your system administrators.

You will also need to involve stakeholders ranging from executive management to program managers for PAM, information security, and identity and access management, as well as integration partners and application and platform owners.

Existing classification tools such as configuration management databases (CMDBs) as well as scanning tools provide a good start but may deliver incomplete or inaccurate results. A formal, hands-on discovery and assessment effort will yield the most accurate information; a discovery effort done with the support of an experienced integration partner can bring best practices to the discovery of your at-risk accounts and assets as well as encourage the required internal co-operation.

STEP 2: IDENTIFY YOUR PRIORITIES

Prioritizing your risks will help you tailor your PAM deployment to give you the highest value return most quickly at an enterprise level. Many organizations skip over prioritizing their risks and move straight into implementation; as a result, they spend too much time focusing on areas or capabilities that don't reduce the most overall risk and deliver the best value to the organization.

For example, an organization might spend months deploying proxies that prevent a group of administrators for a particular system from seeing administrative access passwords and allow the security operations center or PAM team to monitor their sessions. But the organization could have eliminated much more risk more quickly at the enterprise level by implementing password rotation and manual password checkout across multiple teams and platforms.

STEP 3: DESIGN YOUR INFRASTRUCTURE

If you implement PAM correctly, it will become one of your most critical applications, without which much of your everyday business will stop. That means it must be highly available with no downtime. It must also scale to manage even the largest number of active users.

To help meet such peak demands, consider designing your PAM infrastructure in a distributed architecture so the required computing, storage, and networking resources are closest to the accounts and systems under management. Many organizations prefer hosting these assets on-site for greater security but hosting them in the cloud can be an option if the provider offers guaranteed isolation.

As PAM becomes a critical corporate application, ensure high availability with load balanced servers. Create a PAM disaster recovery plan that meets your organization's security requirements, such as the desire of many organizations to keep the backup on-site for maximum control over who can access details about the backup. All PAM backups must assure no downtime and real-time data consistency to ensure a hacker can't use a temporary failure of the authorized process to gain unauthorized access.

Resist the urge to let individual business units or regional areas deploy different versions of your PAM tool. Inconsistent implementations make it harder to enforce common security practices, to add new functionality across the organization, or to move to new architectures such as containers. It also means a user moving to a different business unit or region might need to learn a new interface, which increases training and help desk costs as well as the likelihood of errors.

STEP 4: HARDEN THE INFRASTRUCTURE

Given the criticality of PAM to the organization, the security of the underlying infrastructure deserves special attention. Whether you deploy in-house or in the cloud, pay close attention to how you harden your infrastructure.

First, if an organization employs PAM on-site, it needs to rigorously control which ports traffic is allowed through. Next, the organization may put some components in the demilitarized zone (DMZ), a physical or logical subnetwork separating the corporate network from the Internet and other untrusted networks. Because the DMZ usually limits the number of connections to the internal network, carefully consider which PAM components to put in the DMZ and how they control accounts to ensure availability and compliance with security policies. The PAM configuration in the DMZ will depend, among other things, on the firewall rules in place, licensing requirements, and which protected assets reside on each network. For example, an organization might host only a small subset of its accounts in the DMZ rather than its full vault.

STEP 5: REMEMBER THE BASICS

Before you onboard your first application or account, take basic, effective steps to secure the vault that holds administrative passwords. This is critical because if the vault is compromised, no administrator will trust it, or the rest of your PAM implementation.

Securing the vault requires a number or considerations, including:

□ **Creating separate accounts for users' privileged access and non-privileged access (their access to perform day-to-day business functions).**

□ **Introducing a level of friction in the authentication and access authorization process by introducing multi-factor, risk-based, or adaptive authentication. Single sign-on, while convenient, is not enough proof of identity and can be too easily compromised or spoofed through social engineering methods such as phishing.**

□ **Rotating credentials often, if not on every login (also known as one-time-pass). This will ensure that compromised credentials are of no or limited use to any attacker.**

□ **Ensuring a consistent audit trail for any privileged account activity, with a clear understanding of who is performing what activity at any given time. This is especially important when using shared accounts or credentials.**

□ **Working with your platform owners and administrators to reduce the total number of administrative accounts such as for directory domains and databases. The fewer there are, the fewer you will need to protect and the smaller your attack surface.**

WORKSHEET

5 STEPS TO A STRONG PAM IMPLEMENTATION

Are you wondering where to begin and what it will take to build a strong Privileged Access Management (PAM) implementation that supports your business goals and advances your organization's security? Here are five steps to help you better define, enhance, and protect your PAM investment.

STEP 1: ASSESS YOUR CURRENT STATE

- □ Identify and understand **business goals**
- □ Define **business risks**
- □ Map privileged accounts
- □ Identify key stakeholders

BUSINESS GOALS

____

____

____

____

____

BUSINESS RISKS

____

____

____

____

____

STEP 2: IDENTIFY YOUR PRIORITIES

- □ **Prioritize risks**
- □ Align with business goals
- □ Focus on enterprise-level value delivery

PRIORITIZE RISKS

STEP 3: DESIGN YOUR INFRASTRUCTURE

- □ Ensure high availability with no downtime
- □ Use a distributed infrastructure to help meet peak demands
- □ Create a **disaster recovery plan** with security in mind
- □ Enforce consistency across all business units and regions

DR LOCATIONS	COMPONENT	VERSION	PURPOSE
On-Prem Dallas	PSM	10.4	Active
Data Center VA	CPM	9.8	Warm DR

STEP 4: HARDEN YOUR INFRASTRUCTURE

- □ Control **port traffic**
- □ Assess any PAM components in DMZ and other network zones

PORT NUMBER	DESCRIPTION

STEP 5: REMEMBER THE BASICS

- □ Create separate accounts for users’ privileged access
- □ Introduce robust authentication, such as multi-factor
- □ Rotate credentials often
- □ Ensure a consistent audit trail
- □ Build partnerships with your **administrators**

ADMIN	DEPARTMENT	SYSTEM/APP

GOVERNANCE: THE KEY TO LONG-TERM PAM SUCCESS

Privileged access management (PAM) delivers the greatest benefits when it is implemented as a mission rather than to satisfy a limited, one-time mandate. Achieving more complete and proactive protection for privileged accounts requires an ongoing program to add more platforms and accounts and to share more security data with other systems over time. It also requires paying as much, if not more, attention to how PAM affects people and processes as to technology issues.

Without proper ongoing governance, a PAM program can give an organization a false sense of security regardless of their investment in their initial PAM rollout. Here are the essential elements of ongoing PAM governance, why they are important, and how to get them right.

ONBOARDING

Don’t think of onboarding as something that happens only in your initial PAM implementation. To deliver the maximum benefit, onboarding should be a continuing process that expands the PAM footprint with additional existing systems as well as new platforms as they are acquired by the organization.

The more platforms and accounts you’ve onboarded to your PAM system, the more privileged access you can manage. You can also collect and act on far better information about who is using what accounts, identify your most significant security risks, reduce those risks, and demonstrate your progress to your audit and compliance team.

Organizations often feel they can easily identify their most urgent PAM onboarding needs.

These include systems that support large parts of the business or are most critical for compliance. Identifying the next set of priorities is often more complex because of competing organizational priorities and other factors like imminent upgrades. Despite these challenges, organizations benefit from ongoing prioritization and onboarding efforts, which keep PAM programs aligned with current business needs.

Determining which platforms and accounts to onboard, and when, should include the likelihood of an attack, the business risk from such an attack, and whether the platform is nearing the end of its life and thus might deserve less attention.

Beyond obvious weak points such as systems that are mandated to be remediated, look for those where administrators have failed to close unneeded accounts, were unaware of open accounts, or where audits have shown access requests were not properly reviewed.

TRAINING AND CHANGE MANAGEMENT

As your PAM implementation matures, more administrators will use the PAM tool to access more systems. They will require ongoing training to ensure they adhere to proper PAM processes while being as productive as possible.

We recommend that companies create and maintain training materials and processes to assure scalable, repeatable training programs.

Because the administrators who will use PAM are usually very technical, they rarely require basic training in a tool. Their training should instead focus on making sure they are comfortable with the new PAM processes so that using a PAM tool becomes an essential and routine part of the organization's security practices and culture.

Identifying and educating all the required stakeholders about the benefits of PAM is an essential part of a successful PAM program and helps strengthen the organization's security culture. It is essential to understand the needs of users, how PAM affects how their jobs, and to make reasonable concessions to spur their adoption.

PAM deployments also need the same level of support as any large application rollout: they require familiarity with the business so support staff can identify and educate the right stakeholders, as well as skills in scripting, debugging, support, and upgrades. Your existing operational staff are a valuable resource and likely already familiar with how your organization supports application rollouts.

Train your operational staff on the specifics of your PAM tool and help them build the skills required to maintain your PAM deployment long-term.

INTEGRATION

Achieving true enterprise-wide, ongoing visibility into what your privileged accounts are doing requires integrating your PAM tool with other security tools and processes. These include, among others, security information and event management (SIEM) tools, your security operations center (SOC), and Identity Governance and Administration (IGA) programs. For example, a PAM tool can help the SOC identify which of the flood of alerts it receives each day are most important. Based on input from the IGA platform, suspicious access can be blocked, potentially identifying and mitigating an insider threat.

In particular, the integration of PAM with IGA provides:

□ **Increased enterprise-wide clarity, visibility, and control over access managed through PAM tool**

□ **Easier targeting of privileged accounts for more robust access management**

□ **Reduced operational burden through increased automation of lifecycle events and access requests**

□ **Increased compliance with regulatory requirements through programmatic IGA policies such as Separation of Duties (SOD)**

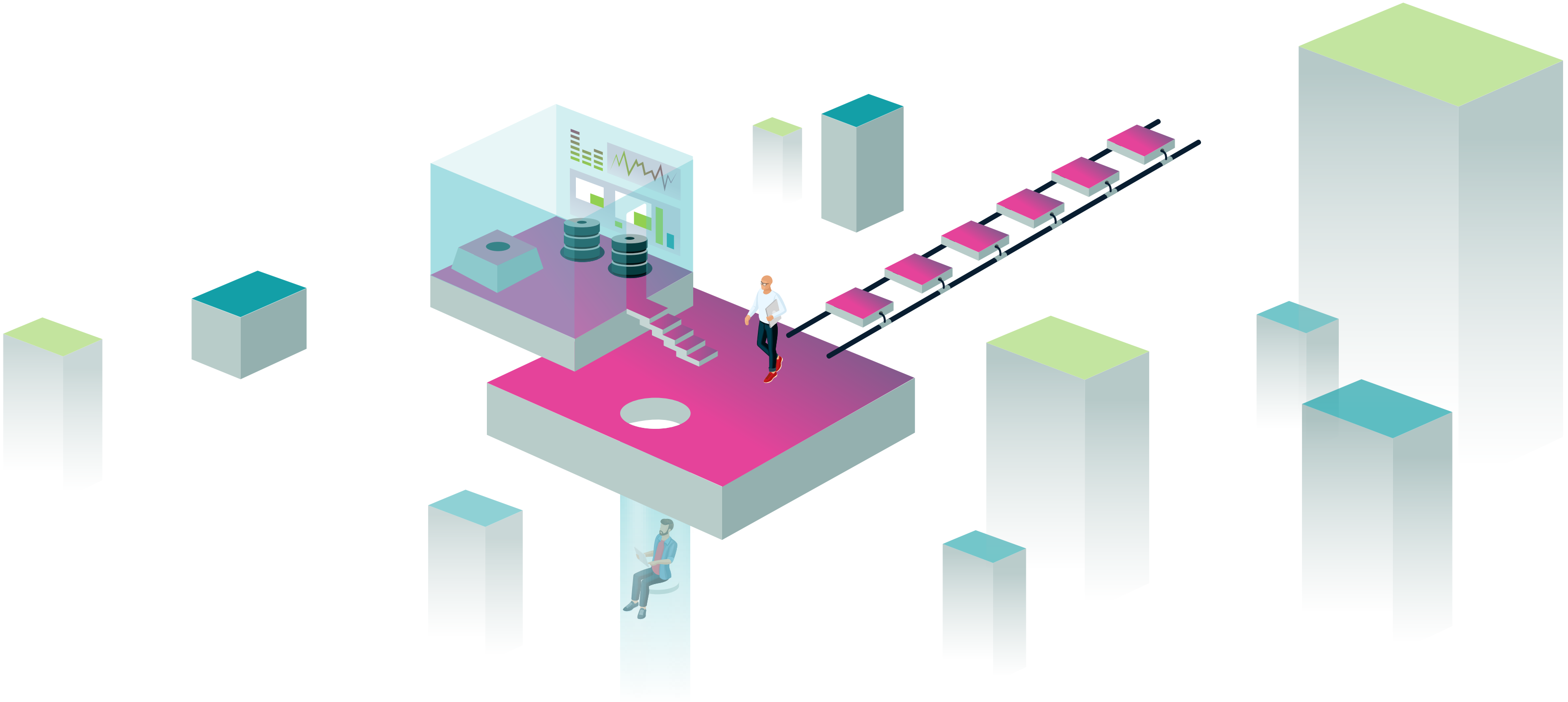
Integration with IGA combined with analytics (described below) allows an enterprise not only to identify suspicious action on a privileged account, but it can also identify other accounts to which an administrator has access. This can provide clues about whether an administrator is acting maliciously, or if their account is under attack from the outside. It can also close an all too common security vulnerability – stale PAM access for users who no longer need it or have left the organization.

ANALYTICS

Performing advanced analytics on the data from mature and well-governed PAM, IGA, and other systems can provide the most proactive, complete, and cost-effective defense against threats as they evolve. While companies should first implement PAM basics such as password rotation and secure password vaulting, they should also plan for scalable, automated analysis of the increasing amounts of usage data they will gather over time. Strong analytics allow you to correlate data from multiple sources to focus attention on the most significant risks.

Analytics help you identify critical situations and take swift, targeted remediation in cases such as:

- □ **Accounts outside the control of IGA and/or PAM tools**
- □ **Overprovisioned accounts**
- □ **Tracking account expiration**
- □ **High numbers of privilege escalation attempts (such as in brute force attacks)**
- □ **Large-volume downloads of sensitive data**
- □ **Logins to critical systems at unusual times or from unexpected locations**



CONCLUSION

WHAT'S NEXT?

In this toolkit, we've described why a mission-driven approach to PAM delivers the highest return on your organization's investment, how to determine if you're ready for mission-driven PAM, how to deploy it, and how to govern and integrate it with other critical systems over time.

Threats from hackers and malicious or careless insiders will not end, nor will demands from regulators and auditors for more thorough and consistent privileged access management. With such high stakes, and the high cost of remediation efforts, a PAM program that meets only point-in-time mandates can increase, rather than reduce, your financial and security risks.

Investing in a broader, ongoing PAM mission delivers the most security at the lowest long-term cost for the most applications and users. To learn more about how to begin your PAM mission, contact the Sila team.

CONTACT INFORMATION

TAPAN SHAH
703.637.8803 | TSHAH@SILASG.COM

TROY REICHERT
312.971.8617 | TREICHERT@SILASG.COM

NOTES

ABOUT SILA

Sila is a technology and management consulting firm that delivers lasting and substantial business solutions to the world's leading corporations and Federal government agencies. Our solutions expertise lies in the areas of cybersecurity, risk management, data analytics, software engineering and integration, strategy and transformation, and digital and creative services.

Deep technical acumen coupled with our proven leadership capabilities enables us to develop solutions that result in long-term value, competitive advantages, and help our clients realize their business goals.

275+ EMPLOYEES NATIONWIDE

HEADQUARTERED IN ARLINGTON, VA WITH OFFICES IN

• SEATTLE, WA • CHICAGO, IL • DENVER, CO • SHELTON, CT

TOP FORTUNE 500 & FEDERAL CLIENTS

95% RATE OF CLIENT RE-ENGAGEMENT