Integrity360

your **security** in mind

Integrity360 Privileged Access Management (PAM) Services

Your ultimate solution for privileged accounts security

Introduction

Did you know that the majority of security breaches involve compromised privileged credentials? Attackers target privileged accounts because they provide unrestricted access to critical systems. Without the right controls, a single compromised admin account can lead to devastating breaches, data loss, and operational disruption.

The challenges at a glance:

- **Credential theft & privilege abuse:** Privileged accounts are prime targets for attackers; compromised credentials can lead to full system takeovers, data breaches, and ransomware attacks.
- **Lack of visibility & discovery of privileged accounts:** Many organisations struggle to identify all privileged accounts, credentials, and embedded secrets across their environment. Unmonitored or orphaned accounts create security blind spots and increase the attack surface.
- **Balancing security with user productivity:** Excessive security controls can frustrate users and slow down operations. Organisations struggle to enforce least privilege without disrupting legitimate administrative workflows.
- **Compliance & regulatory challenges:** Regulations like GDPR, NIS2, and ISO 27001 require strict privileged access controls and audit trails. Failure to meet these standards can lead to penalties and reputational damage.
- **Complexity & cost of deployment:** Traditional PAM solutions can be difficult to deploy and manage, requiring significant internal expertise and resources—making it challenging for many organisations to maintain and optimise.

Compromised privileged identities accounted for 33% of security incidents in the 2024

– Identity Defined Security Alliance (IDSA) report, 2024

Adopt the right Privileged Access Management strategy with Integrity360:

Integrity360 offers a range of Privileged Access Management (PAM) Services including consultancy, implementation, and managed service, providing a flexible approach where organisations can choose the right level of support based on their needs.

The increasing importance of PAM

There are many factors that increased the importance of adequate governance and control of privileged access.

- **Identity-first Security** is a security approach that places user and entity identity at the centre of the security strategy
- As a result of Work-From-Anywhere and cloud adoption, identity has become **the main perimeter,** the key attack surface and the ultimate control surface, and the first pillar of Zero Trust security model
- **Privileged Access Management (PAM**) is one of main crucial areas of IAM, focusing on securing privileged sessions, accounts, and activities

Staff, vendors, and other insiders have unnecessary or over permissive access to systems and data. Passwords are created and shared, but are not audited, monitored nor managed with discipline and accountability. Endpoints, workloads, servers and applications communicate and open paths to sensitive assets and data - to name a few - causing complexity, increasing risk and creating weak points that can be exploited or abused.

PAM technology overview

Privileged Access Management (PAM) is the discipline that includes procedures and technologies to control the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. Common capabilities include credentials management, and session management, recording and proxying. Below are the main categories that represent the required capabilities of modern, efficient PAM solutions:

- **Privileged Account and Session Management (PASM):** PASM focuses on securing, managing, and monitoring privileged accounts and their sessions. It involves vaulting credentials, brokering access, and recording sessions to ensure controlled and audited use of administrative privileges. This approach helps prevent unauthorised access and provides a comprehensive audit trail for compliance purposes.

- **Privilege Elevation and Delegation Management (PEDM):** PEDM provides granular control over user privileges by allowing temporary elevation of access rights and delegation of specific tasks. This ensures users have only the necessary permissions for their roles, reducing the risk of over-privileged accounts and enhancing security. PEDM solutions often include host-based command control and privilege elevation for servers, enabling specific commands to run with elevated privileges without granting full administrative access, that's why it's also known as Endpoint Privileges Management (EPM).

- **Remote Privileged Access Management (RPAM):** RPAM secures remote access for external IT workers by enabling them to authenticate and access privileged systems without the need for traditional VPNs. This is achieved through a PAM gateway that brokers authorised access, ensuring that remote sessions are secure and monitored. RPAM solutions often include features like desktop sharing, credential vaulting, and session recording to maintain security and compliance during remote access.

- **Secrets Management:** Secrets Management involves the centralised handling of sensitive credentials such as passwords, API keys, SSH keys, and certificates used by applications, services, and machines. By programmatically managing, storing, and retrieving these secrets through APIs and SDKs, organisations can enforce consistent security policies and ensure that only authenticated and authorised entities access critical resources. This practice is essential in dynamic environments like DevOps and cloud-native applications, where automated processes require secure access to resources.

- **Just-In-Time Privilege (JITP):** JITP grants users temporary, time-bound privileged access to perform specific tasks, minimising the risks associated with standing privileges. This approach ensures that elevated permissions are active only when necessary and are automatically revoked afterward, reducing the window of opportunity for potential misuse or attacks. Implementing JITP is a critical component of a robust PAM strategy, aligning with the principle of least privilege and enhancing overall security posture.

Our methodology

Stage 1 | Discover and assess

In this phase, we aim to answer key questions: **What we can find?** (Scanning and assessment) **| What do we know?** (Processes and business logic) **| What is the risk?** (Findings) **| How do we secure it and optimise it?** (The roadmap).

We identify the organisation's current state through assessment, technical scans, and interviews to capture the AS-IS state. Our consultants will highlight the top risks and develop a roadmap document to discuss with the customer's stakeholders to agree priorities and refine the roadmap to achieve the required TO-BE state.

Stage 2 | Design and build

In this phase, we move to the actual architecture of the PAM solution, considering all the technical and business requirements, including integrations, authorisation workflows, roles and responsibilities, exceptions, resilience, and other several factors to ensure the optimum PAM solution design.

Once the architecture is agreed, we start the deployment and build process to deliver the PAM solution, ensuring it's operational and functioning as designed.

Stage 3 | Develop and onboard

This stage focuses on workflow development and implementation, securing the scoped credentials, secrets and accounts in the safe, defining compliance needs and reducing the overall risk, following a "low-hanging fruit" approach, mitigating the top risks with the least number of actions.

This is considered the foundation that will evolve to a repeatable process, to gradually extend PAM usage to more accounts, teams and use cases.

Stage 4 | Manage and expand

Here the goal is to reach BAU state, where PAM workflows should be considered when rolling out any new project to prevent the need to re-design the future onboarding process, providing clear guidance and onboarding process.

In this stage, we usually start focusing on team-specific issues and exceptions that require custom or ad hoc integrations, expanding the PAM use cases and workflows to cover more authorisation workflows.

Once a repeatable process is defined and operated, we expand the PAM use cases to cover accounts like network devices, console accounts, and other accounts. We also enable more advanced features such as session terminations and isolation criteria, integration with SIEM/MDR or ITSM systems, delivering end users training and Standard Operating Procedures documentation.

Stage 5 | Harden and optimise

Now, as a consistent and reliable BAU state has been achieved, we can investigate more advanced and complex use cases. We consider questions such as:

Do all applications and scripts in the business have their passwords rotated with the PAM solution?

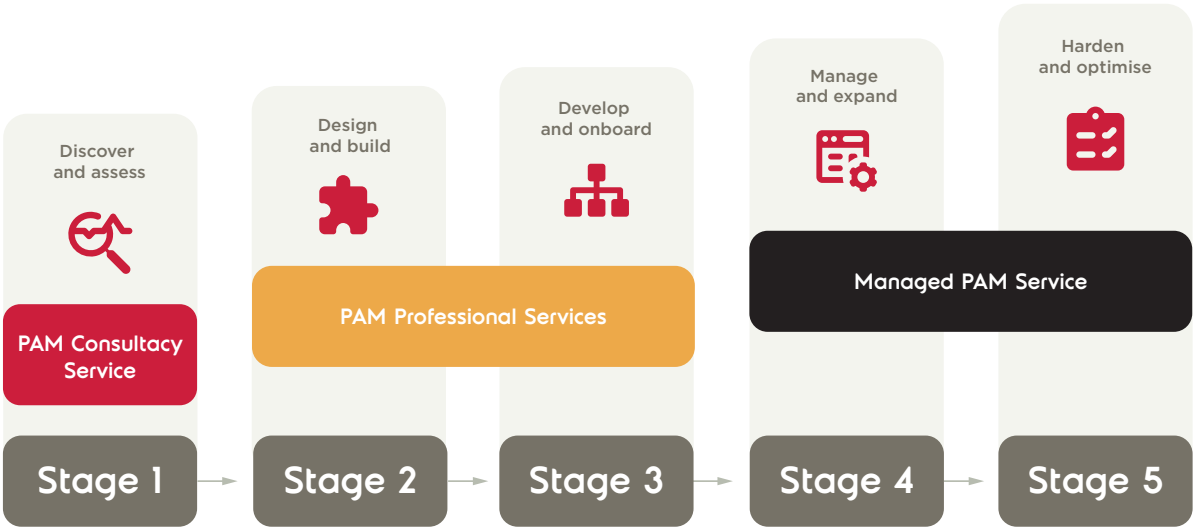
What process do outside contractors (3rd party) use to enter the environment?

Can we prove that Least Privilege is enforced across the business?

Using our battle-tested PAM methodology, we ensure consistent outcomes, improved operational efficiency and driving higher technology-adoption rate across our clients' estate.

Our PAM Services

Integrity360 offers a range of Privileged Access Management (PAM) Services including consultancy, implementation, and managed service, providing a flexible approach where organisations can choose the right level of support based on their needs.



PAM Consultancy Service

Our PAM consultancy package enables organisations to discover their privileged accounts risk, develop a risk-based strategy to adopt or improve PAM technology, and create business processes to streamline authorisation workflows. The goal of this service is to produce PAM strategy that is driven by a functional roadmap, based on our flexible and adaptable maturity index model, and should be viewed as a starting point for all PAM initiatives within organisations of all sizes. A strategic vision and a plan for the implementation of an enterprise-wide PAM programme is defined within our PAM consultancy engagement and roadmap. The PAM Consultancy Service covers stage 1 in our PAM methodology.

PAM Professional Services

Our expert-led Professional Services ensure the design, build, development and accounts onboarding of your PAM solution. We help organisations implement robust security controls while minimising complexity and operational disruption, covering stages 2 and 3 in our methodology.

Managed PAM Service

Our managed PAM Security Service safeguards your most critical accounts, ensuring only the right people have the right access at the right time. With expert monitoring and analysis, scalability, and robust management and support, we help our clients prevent breaches, mitigate insider threats and fulfil compliance requirements. Our experts take the complexity out of PAM, delivering seamless protection, streamlined access governance, and deliver value aligned with the business goals. Our managed service is aligned with our methodology, focusing on stages 4 and 5.

Our Managed PAM Service features

Our Managed Security Service (MSS) team takes care of all operational security tasks, from policy development to managing exclusions and exceptions. We ensure your security technologies stay up to date by handling upgrades and patching, keeping your defences strong and compliant.

Acting as an extension of your operational support team, we work in partnership to align security services with your business needs. Our approach enhances operational efficiency by delivering consistent, reliable, and anticipated outcomes.

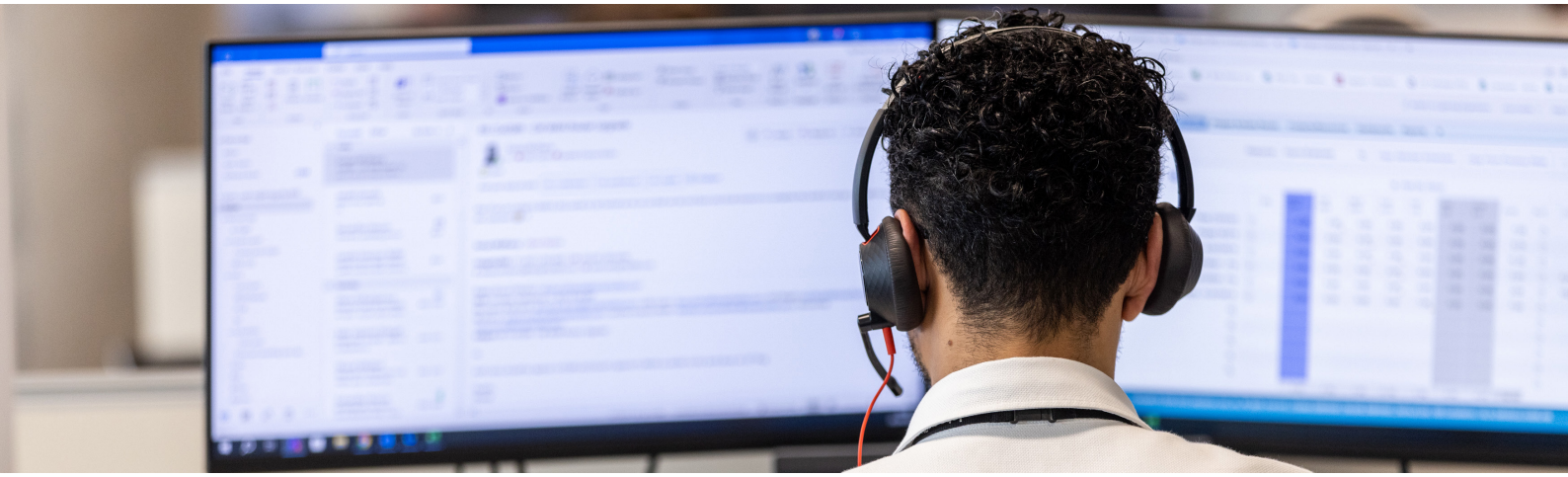
With built-in flexibility, we adapt to evolving business requirements and changes in workload, responding quickly and effectively. Whether it's optimising security processes or addressing new challenges, Integrity360's MSS team is committed to delivering value while reducing the burden on your internal teams.

Summary of the managed service deliverables

- ✓ Remote management and support service
- ✓ System maintenance and updates
- ✓ Policy and change management
- ✓ Account onboarding and maintenance
- ✓ Prioritised onboarding plan development
- ✓ Standard and custom reporting
- ✓ Daily health checks
- ✓ Monthly review report
- ✓ Monthly review workshop
- ✓ Annual As-Built documentation

Your security, our priority

With Integrity360's PAM Services, safeguarding your privileged accounts becomes an integrated process. Our experts take the complexity out of PAM, delivering seamless protection, streamlined access governance, and deliver value aligned with your business goals.



Why choose Integrity360?

Choosing a cyber security provider is a critical decision for any business. Here are just a few reasons why you should choose Integrity360:

- **Passion & commitment:** We are passionate about cyber security and committed to delivering the best possible protection for our clients' businesses.
- **Certifications:** Greatest level of technical certifications and capability.
- **Partnerships:** Strongest vendor partnerships and support arrangements.
- **Recognition:** Recognised by Gartner in multiple market guides.
- **Six Security Operation Centres (SOC)** located in Ireland, Spain, Italy, Sweden, Bulgaria and South Africa.
- **Experience:** With over +500 security consultants, engineers, and analysts, we have the global experience and expertise to safeguard your business from even the most complex and evolving threats.
- **Reputation:** We have earned the trust of thousands of global companies and have a strong reputation in the industry, built upon by exceptional technical expertise, a client first attitude, and a proven track record on complex security projects.
- **Customised solutions:** We take a personalised approach to cyber security, partnering closely with each client to understand their unique needs and recommend the most effective security solutions.

integrity360.com
info@integrity360.com

London, UK
+44 20 3397 3414

Kyiv, Ukraine
+38 0 504 701 125

Stockholm, Sweden
+46 8 514 832 00

Dublin, Ireland
+353 01 293 4027

Madrid, Spain
+34 910 767 092

Sofia, Bulgaria
+359 2 491 0110

Zurich, Switzerland
+34 910 767 092

Ludwigsburg, Germany
+49 7141 48799 80

Cape Town, South Africa
+27 21 100 3774