



PRIVILEGED ACCESS MANAGEMENT (PAM)



IBM Privileged Access Management (PAM) is a critical security solution designed to protect organizations from threats associated with privileged accounts. By enforcing strict access controls, monitoring privileged sessions, and ensuring that privileged credentials are managed securely, IBM PAM reduces the risk of unauthorized access to critical systems and data. This solution is tailored to meet the complex needs of modern enterprises, providing comprehensive protection and compliance with regulatory requirements.



KEY FEATURES

- **Access Control**
Enforces robust policies to limit and control access to privileged accounts, ensuring that only authorized users can access sensitive systems.
- **Session Monitoring**
Continuously monitors and records privileged sessions to detect and respond to suspicious activities in real-time.
- **Credential Management**
Securely stores and manages privileged credentials, automatically rotating passwords and keys to prevent unauthorized access.
- **Audit & Compliance**
Provides detailed logs and reports for audit purposes, helping organizations demonstrate compliance with regulations such as GDPR, SOX, and HIPAA.
- **Integration**
Seamlessly integrates with existing IT infrastructure and security tools for a unified approach to access management.

KEY BENEFITS

- **Reduced Risk**
Mitigates the risk of insider threats and external attacks by securing privileged accounts and limiting access to critical resources.
- **Enhanced Security Posture**
Strengthens overall security by ensuring that privileged access is tightly controlled, monitored, and audited.
- **Regulatory Compliance**
Simplifies the process of meeting regulatory requirements with comprehensive audit logs and compliance reports.
- **Operational Efficiency**
Automates credential management and access controls, reducing administrative overhead and minimizing human error.

KEY DELIVERABLES

- **Secure Privileged Access**
Implements robust security measures to protect privileged accounts and sensitive data from unauthorized access.
- **Real-Time Threat Detection**
Provides real-time monitoring and alerts for any suspicious activities related to privileged accounts, enabling prompt response.
- **Compliance Support**
Delivers the tools and reports needed to achieve and maintain compliance with industry regulations.
- **Scalable Protection**
Adapts to the needs of your organization, scaling to accommodate the growing complexity of modern IT environments.