Privileged Access Management (PAM) is the monitoring and protection of privileged (super user) accounts in an organization’s IT environment, which are the most common targets of attack.

PAM is a holistic set of technologies and processes designed to create, modify, control access to and terminate privileged access.

Oversight is necessary so that the greater access abilities of super user accounts are not misused or abused.

Why You Need It

Privileged Access Management (PAM) is the monitoring and protection of privileged (super user) accounts in an organization’s IT environment, which are the most common targets of attack.

PAM is a holistic set of technologies and processes designed to create, modify, control access to and terminate privileged access.

Oversight is necessary so that the greater access abilities of super user accounts are not misused or abused.

How You’ll Benefit

» Risk Reduction: Protect sensitive access to critical devices and systems where users may leak confidential information, change transactions and remove audit trail.

» Policy Improvement: Enable continuous and sustainable policy enforcement over administrative and root accounts across the organization, ensuring established business and security policies are continuously followed.

» Compliance Alignment: Detect, monitor and report on privileged account activity, improving the audit process and meeting compliance guidelines.

» Visibility Improvement: Identify and monitor both privileged accounts and their usage.

Success Story

This Top 10 Investment Bank in the World had an immediate need for 24/7 operations and support. They lacked the processes necessary to manage their huge number of privileged accounts from their infrastructure. They also suffered a poor state of security control. Their helpdesk, branch support professionals, and auditors experienced many problems trying to perform their own tasks as well as some difficulties in investigation of incidents.

With Simeio Solutions, this investment bank achieved:

» Successful migration to new IAM: 3.2 million external identities lined up for end-user (citizen) self service. With an SLA based operational support, achieved 99.9% availability.

» Controlled & On-demand elevation to temporary administrative access for employees. Resulted in huge improvement in productivity, helpdesk tickets, and compliance.

» Simeio defined and implemented emergency access or “Break glass” process for 50 business critical financial applications. Additionally, provided Jefferies a hassle-free tool for managing all vendor support tickets in one place.

» As the Jefferies’ preferred IAM advisor, Simeio introduced industry standards and best practices for IAM, PAM and VD services and processes.
Our Connect and Protect Focus gives you a complete range of customized solutions, proven effective for over 150M+ identities. Get #SimeioSafe

### Identity Administration
Simeio can manage your end-to-end identity lifecycle for employees, partners, customers and devices. We’ll handle all account requests, resets and access termination.

**Business Problems Solved:** Faster onboarding and offboarding, better controls, compliance and cost improvements through automating manual processes and automated access termination.

### Access Governance
Let Simeio automate compliance and protect your enterprise against threats with solutions for access certifications, segregation of duties enforcement, role management, and identity proofs.

**Business Problems Solved:** SOX compliance, time-consuming manual access review, reduce audit findings or compliance violations.

### Access Management & Federation
Get peace of mind and much more secure authentication. Simeio can implement a seamless single sign-on (SSO) to any on-premise application or network resource. Enjoy secure access from any device, supporting all federation standards. Educate your business on the risks, all while building your business.

**Business Problems Solved:** Too many sign-ons, frustrating user experience.

### Data Security and Loss Prevention
Security solutions for all types of databases as a hosted managed service. Set up policies to discover and prevent unwarranted actions on your sensitive content and data in the cloud. Centrally manage and enforce data management policies, alerts, logs and data egress blocking.

**Business problems solved:** Ensuring that private data remains private.

### Security & Risk Intelligence
Deploy and maintain security and behavioral analytics with Simeio. User and entity behavioral analytics can deliver continuous risk monitoring. Sophisticated machine learning algorithms enable real-time detection of breaches and threats.

**Business problems solved:** Ensuring that people are using their access appropriately.

### Privileged Identity Management
Now you can securely manage passwords & SSH keys for SaaS and on-premise applications through auto-discovery, privileged checkout, session recording & threat analytics. Simeio will automate compliance reporting with integration to existing access governance & MFA.

**Business Problems Solved:** Identifying privileged access, reduced risk by improved controls, integration of privileged accounts into governance platform.

### Core Directory Services
Simeio can help you manage your identities on a global scale, with high performing and flexible virtual directory solutions. Enable secure and seamless access to web and cloud solutions and directory management.

**Business Problems Solved:** Single view of identity in highly complex environment to enable secure and seamless access to web and cloud solutions, giving right access at any time with any device.

### Cloud Security
Protect critical cloud infrastructure with Simeio Solutions that can detect shadow IT. Automate cloud security admin, including SaaS end-to-end control through real-time cloud threat intelligence.

**Business problems solved:** Reduction in Shadow IT and improved security around employees use of the internet.