Grant Thornton PAM Services

Connect Everything. Securely.

Saviynt

Grant Thornton

Problem Statement

As organizations grow and incorporate both human and non-human elements, expanding their IT resources for business operations, privileged access management becomes increasingly critical for security and compliance. Organizations seek efficient methods to centralize privileged access management across their IT environments and implement advanced security measures to address the heightened risks associated with privileged accounts.

Grant Thornton has implemented Saviynt's Privileged Access Management capabilities to secure privileged access and protect critical assets throughout their entire infrastructure. This minimizes clients' IAM security risks, ensures compliance, and simplifies auditing. The PAM solution provided by Grant Thornton and Saviynt offers centralized protection for privileged accounts across both on-premises and cloud infrastructure servers. Additionally, it streamlines the management of access to network devices and critical enterprise applications.

Customer Value

Our quick start Privileged Access Management package solution secures privileged access and protects critical assets across your entire infrastructure. It provides fine-grained privileged access management across

all applications to enable the adoption of the Zero-Trust Principle based on real-time risk detection. This solution effectively implements and allows the Saviynt PAM feature and other services for a comprehensive approach to IAM security.

- Identify the organization's privileged access management challenges and gaps to improve the protection of valuable assets and privileged accounts.
- Offer a quick-start PAM package to demonstrate time-to-value and cover use cases for seamless Windows, Linux, and database server onboarding.
- Provide comprehensive support for onboarding various network devices, such as switches, routers, and firewall devices, enabling seamless access via credential-less and just-in-time (JIT) access.
- Enable real-time monitoring of user activities through keystroke logging, recording input and output for each session into searchable records to support audit data using Saviynt.
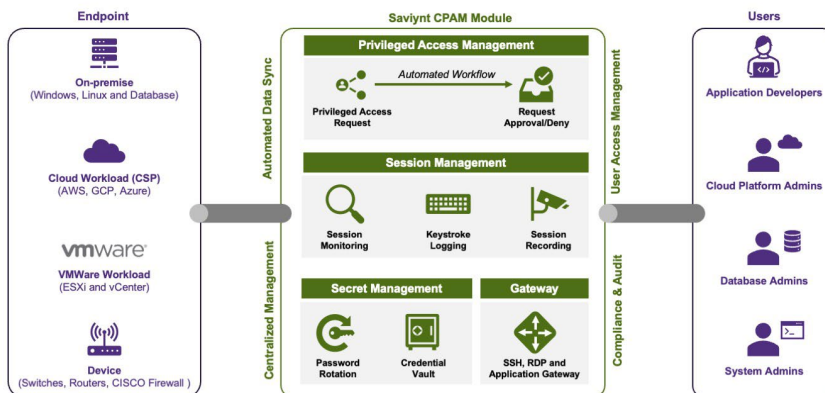
The diagram below illustrates how users grant privileged and endpoint access using PAM modules, along with their key benefits:

- Automatically discovers and controls both on-premises and cloud workloads.
- Provides real-time discovery of new privileged accounts to help detect and control the creation and elevation of high-privilege accounts on endpoints.
- Secures access to and storage of privileged shared credentials in a credential vault that stores critical server and application credentials.
- Enhances privileged account security by periodically rotating passwords for shared privileged accounts and high-privilege connection credentials.
- Saviynt's PAM solution is delivered via an agentless, zero-touch cloud architecture, quickly deploying privileged access capabilities, achieving zero-standing privileges with just-in-time access, and providing intelligent risk insights.
- Provides video (session) recording of user activity, keystroke logging, and session analytics to identify risky activities in recorded sessions.

Use Cases

- Implemented PAM through an agentless, zero-touch cloud architecture, achieving zero-standing privileges with just-in-time access and providing intelligent risk insights using Saviynt's PAM solution.
- Integrated the Active Directory domain, servers, and onboarded service accounts to manage special accounts via PAM.
- Implemented a Privileged Account Management session to request and manage access to privileged accounts and passwords with time-bound access.
- Onboarded on-premises and cloud servers with PAM, including Windows, Linux, AWS, GCP, and Azure.
- Onboarded VMware ESXi and vCenter servers within PAM and enabled password less authentication to access the server via a remote application using the Saviynt cloud console.

- Integrated network devices, including switches, routers, and firewall devices, enabling seamless authentication to access those devices using a secure hashing key.
- Implemented Azure VM management via a centralized console through PAM.
- Enabled real-time discovery of new privileged accounts to help detect and control the creation and elevation of high-privilege accounts on endpoints.
- Integrated secure access and storage of privileged shared credentials in a credential vault that stores critical server and application credentials.
- Integrated session recording of user activity, keystroke logging, and session analytics to identify risky activities in recorded sessions.

Solution Benefits

Grant Thornton offers a quick-start Privileged Access Management (PAM) service to prevent the misuse of privileged access by streamlining the authorization and monitoring of privileged users. This service is delivered through an agentless, zero-touch cloud architecture for fast and secure deployment. By combining Saviynt's advanced technology with Grant Thornton's expertise, clients benefit from streamlined privileged access management, automated machine discovery with robust security controls, and enhanced regulatory compliance assurance. Grant Thornton provides customized solutions to help organizations efficiently manage special accounts and workloads, improving operational performance. The company strengthens its client services by assisting businesses in confidently and efficiently managing privileged accounts.

Cloud Privileged Access Management (CPAM)

ABOUT PARTNER

Grant Thornton Advisors LLC is the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL is an international umbrella entity composed of independent member firms with over 700 offices across 130+ countries. It is represented by more than 68,000 personnel worldwide and is structured with individual country partnerships, much like the Big Four member-firm structures. GTIL does not operate an "alliance" or "affiliate" network — a structure used to supplement a global network utilized by some "global" firms. Instead, Grant Thornton member firms use the same methodologies and innovative technology platforms and share a joint commitment to personalized, seamless client service. GTIL and each member firm are separate legal entities.

Visit GT.COM for more information about the provider.

Next Steps

- View the extensive library of integrations at https://saviynt.com/integrations to see detailed information and implementation guides designed to help you get the most from the Enterprise Identity Cloud.

ABOUT SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt

Headquarters, 1301 E El Segundo Bl, Suite D, El Segundo, CA 90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com