Seamless Security

Unifying IAM & PAM For Identity-Centric Access Management And Workflow Approvals

The power of two: IAM & PAM Governance

In collaboration with SSH, we've built a platform that seamlessly integrates:

- IAM's powerful identity and access governance (MFA, SSO, etc.) and entitlements
- PAM's RBAC, access surveillance, session recording, and auditing
- Ticketing and approval workflows with seamless ServiceNow integration

appmore.com

appmore

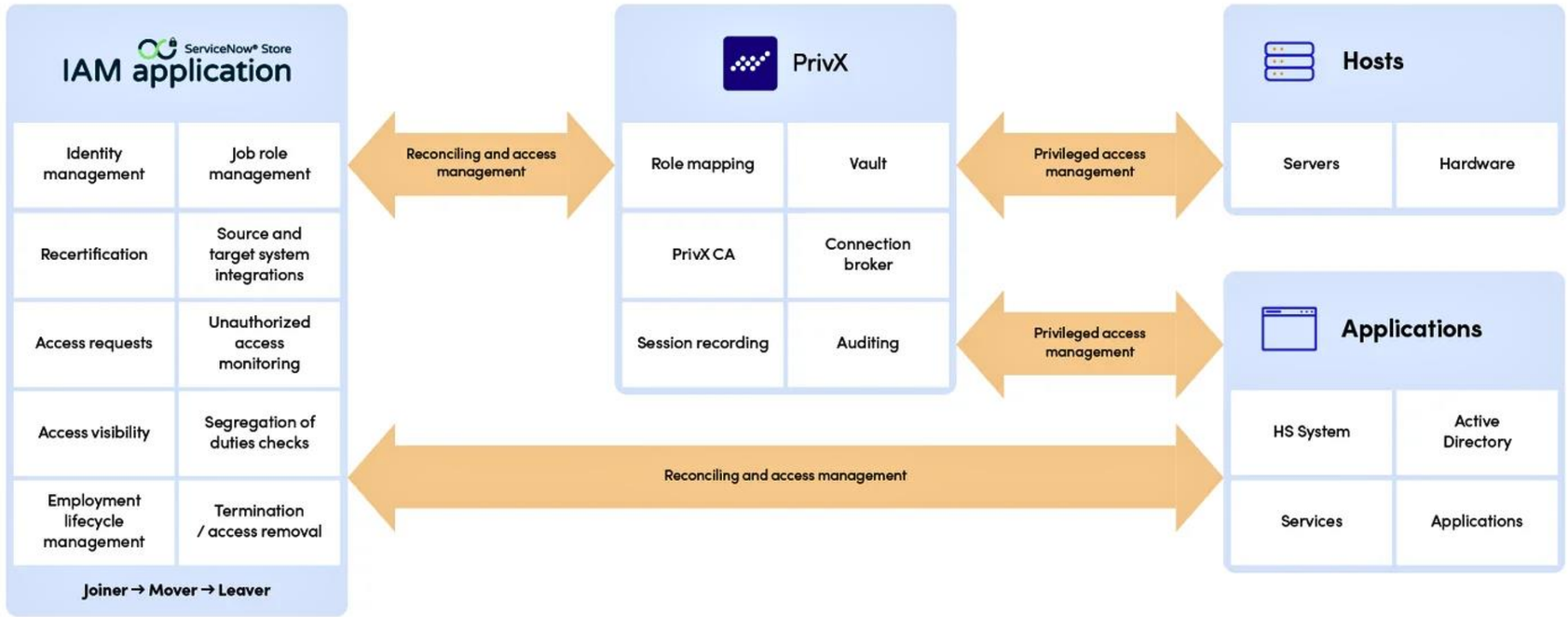
Solution overview

A unified Identity and Access Management (IAM) along with Privileged Access Management (PAM) solution provides a comprehensive security approach, merging the strengths of IAM and PAM into a singular platform. By merging IAM's management of user identities and PAM's oversight of privileged accounts and access, organizations can attain a complete perspective and authority over who can access their resources and crucial data, the extent of their permissions, and the timing of such access.

The integration of IAM and PAM facilitates the centralization and streamlining of processes related to identity and user access. Simultaneously, an IAM-PAM solution serves as the sole control point for these processes, simplifying the overall management of identity, access, and accounts.

appmore

How does it work?



4-step process

• Access Request and Authorization

- Users initiate access requests through Appmore's ServiceNow application.
- Administrators can efficiently authorize access based on predefined roles.
- The application eliminates the reliance on email or outdated solutions for managing access requests. HR processes for new hires, internal transfers, and departures can seamlessly integrate with identity and privileged access management.

2. Passwordless Authentication

- Users are encouraged to employ passwordless authentication methods, such as biometric authentication whenever possible.
- In instances where traditional credentials like passwords or keys are necessary, they can still be utilized, securely vaulted, regularly rotated, and managed appropriately.

3. Access Monitoring and Compliance

- The solution equips users with essential tools to adhere to access requirements stipulated by regulations like GDPR, ISO27K1, and PCI DSS.
- Access is automatically revoked in the event of anomalies during a session, such as the disabling of antivirus solutions.

4. Automatic Access Revocation

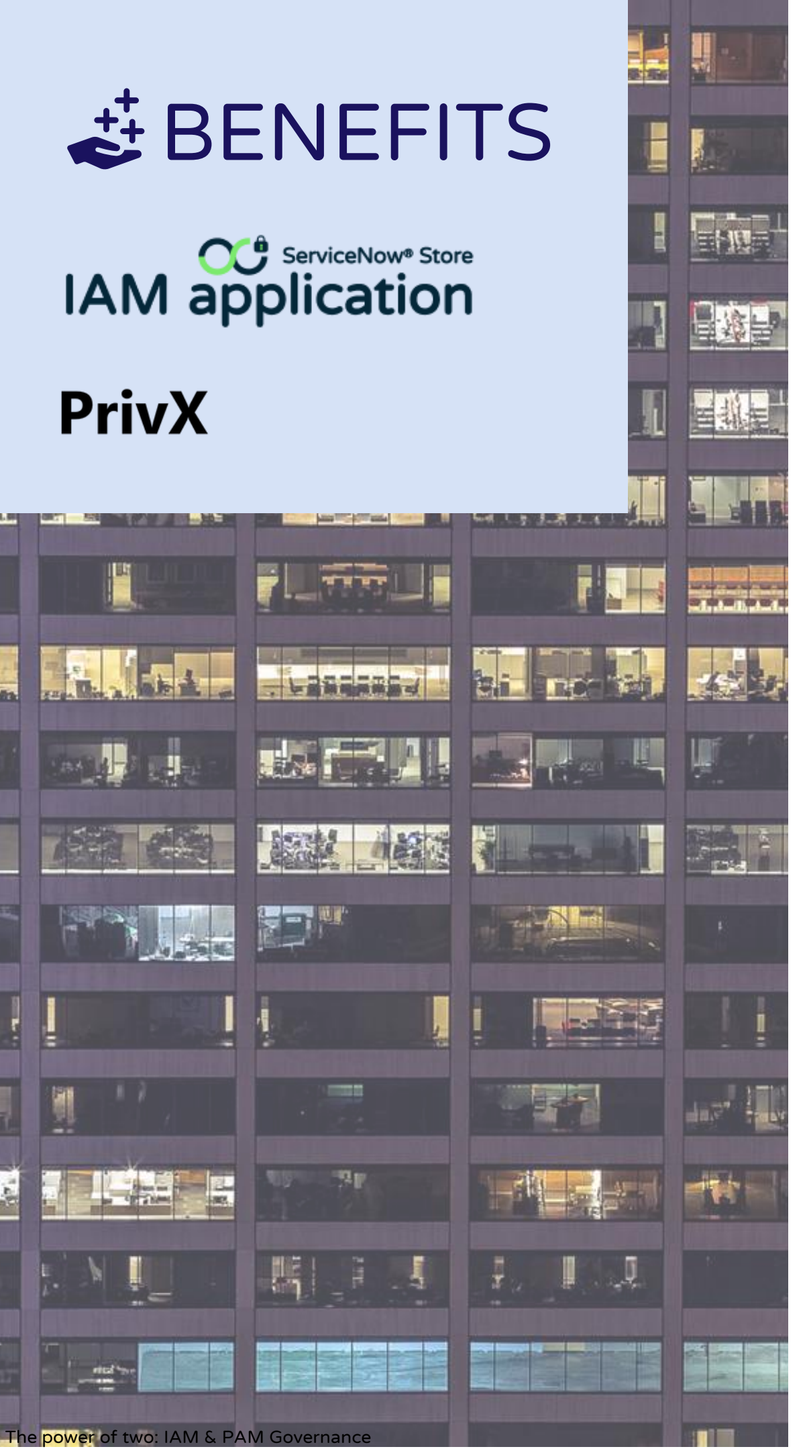
- Upon an employee's departure, the IAM application orchestrates the deactivation of user accounts and the removal of all access rights.
- Due to synchronization between PAM and IAM, all access privileges are revoked simultaneously.
- Every action, including requests, additions, authorizations, and removals, is meticulously traced and logged.

appmore

BENEFITS

ServiceNow® Store
IAM application

PrivX



Request access and assign permissions based on roles

- Role-Based Access Control (RBAC) is facilitated through SSH's PrivX Privileged Access Management (PAM), leveraging roles automatically provisioned by Appmore's integrated Identity and Access Management (IAM).
- Users have the convenience of effortlessly requesting access, and such requests are automatically approved based on the permissions associated with their designated roles.
- Administrators can readily provide temporary or permanent access aligned with specific tasks, projects, or other criteria.

Reduce the risk of unauthorized access

- The system autonomously identifies irregularities in sessions (e.g., PAM bypass) and reports them.
- If there's a breach of company policy, the solution automatically withdraws access, even if users possess otherwise valid credentials.

Effortless workflow authorizations

- Take advantage of automated support for the joiner-mover-leaver process, even involving third parties.
- As employees join, transition, or exit projects following HR procedures, this strategy guarantees the precise provisioning, adjustment, or removal of access as required.

Meet the criteria for Segregation of Duties (SoD)

- This helps avoid scenarios like granting test-to-production access or approving invoices for the same individual.
- Such prevention is a fundamental necessity aligned with various regulatory standards and processes, including PCI DSS.

Secure compliance with regulatory obligations

- Every action, be it a request, addition, granting, or removal, is traced and logged, making user role recertification an integral component of the solution.
- This guarantees that the privileged and other rights align with the roles assigned to specific user(s) and comply with regulatory requirements.

Empower complete password-free authentication

- Provide passwordless access seamlessly just-in-time for the session, ensuring users never encounter or manage the secrets required to establish connections.
- Implement methods such as biometric authentication and single sign-on (SSO) to construct a passwordless pathway for your users.
- This approach is not only convenient but also enhances security and operational efficiency.

appmore

ServiceNow IAM by Appmore

The ServiceNow application optimizes IAM and IGA (Identity Governance and Administration) procedures, introducing a governance and administration layer for all identities and access to elevate your overall IAM experience.
A standout feature of this application is its automation prowess, leading to significant reductions in operational costs and heightened efficiency. From ordering access rights to approvals, creation, and removal, the application seamlessly streamlines the entire lifecycle of identity and access processes.

Moreover, the IAM application equips you with essential tools to align with access requirements outlined by GDPR, ISO27K1, and PCI DSS. Its user-friendly interface and robust reporting capabilities provide comprehensive visibility into all user accounts and accesses within target systems. This includes information on those who initiated and approved these actions. The application facilitates access reviews for accounts and access rights, incorporating segregation of duties checks to aid in successfully passing both internal and external audits.

Users can effortlessly request various access rights via ServiceNow's service portal, eliminating the need for traditional email or legacy solutions in handling access requests. Both users and managers can request indefinite or temporary roles and promptly remove unnecessary access when it becomes obsolete.
Upon an employee's departure, the IAM application proficiently manages the deactivation of their accounts and removal of all associated access rights, significantly enhancing overall security. Additionally, the application allows for the deactivation of a user's account during extended leaves, with the flexibility to reactivate it upon the user's return, adding an extra layer of security.
To sum up, the IAM application for ServiceNow stands as a robust solution for elevating access and identity management, enhancing security measures, and seamlessly aligning with regulatory compliance requirements.

PAM PrivX by SSH

PrivX stands out as a scalable, cost-effective, and highly automated hybrid Privileged Access Management (PAM) solution designed to support hybrid and multicloud environments. This solution enhances both security and operational efficiency by providing centralized access to critical targets for superusers and privileged users, all without leaving behind any credentials. With PrivX, management of access to on-premises, hybrid, or cloud environments is consolidated under a single platform.

PrivX facilitates a smooth transition to secure and cost-efficient passwordless authentication. It accommodates password vaulting and rotation when necessary, enabling businesses to migrate at their own pace. In the PrivX Zero Trust model, connections are established using ephemeral certificates generated just-in-time for a session and automatically expire shortly afterward. This approach leaves no credentials behind to manage, lose, share, or rotate.

Furthermore, PrivX seamlessly syncs with Active Directory, automatically mapping existing identity groups. Users are then granted access based on their roles through Role-Based Access Control (RBAC), rather than individual identities. PrivX ensures that users receive precisely the right amount of access at the right time, for the right duration, and with the appropriate level of privilege through automated processes.

Appmore

Appmore specializes in delivering and overseeing business applications, driven by a mission to provide maximum value to its customers. The paramount focus at Appmore is customer satisfaction, and every team member diligently strives to understand and meet customers' genuine needs in an agile and responsive manner.

The commitment to delivering exceptional customer service is deeply ingrained in Appmore's approach, which revolves around tailoring solutions to meet the unique requirements of each individual customer. The ultimate goal is to offer a seamless and customized experience aligned with the specific business needs of customers.

With an extensive track record spanning well over a decade, Appmore has successfully served numerous customers, completing hundreds of projects related to ServiceNow and Identity and Access Management. Throughout this journey, Appmore has consistently received high praise for both customer and employee satisfaction.

appmore.com

SSH

SSH is a defensive cybersecurity company with a mission to secure critical data and communications between systems, automated applications, and people. SSH product portfolio is developed to defend business secrets and access to them – now and in the future. With SSH teams in North America, Europe, and Asia along with a global network of certified partners – SSH is the pioneer in secure communications serving customers for 25+ years. From large financial institutions and governments to operational technology and critical infrastructure. The company’s shares (SSH1V) are listed on Nasdaq OMX Helsinki.

ssh.com

appmore

Ignite Your Workflows