Solution brief

Identity-based security & access management

A powerful solution combining the best of IAM, PAM, and workflow approvals.

The best of both worlds:
IAM & PAM convergence

A converged IAM (Identity and Access Management) and PAM (Privileged Access Management) solution offers a comprehensive approach to security that combines the best of IAM and PAM into a single platform. By combining IAM's user identity management and PAM's privileged accounts and access management organizations can get a holistic view into and control over who has access to their resources and critical data, with what rights, and when.

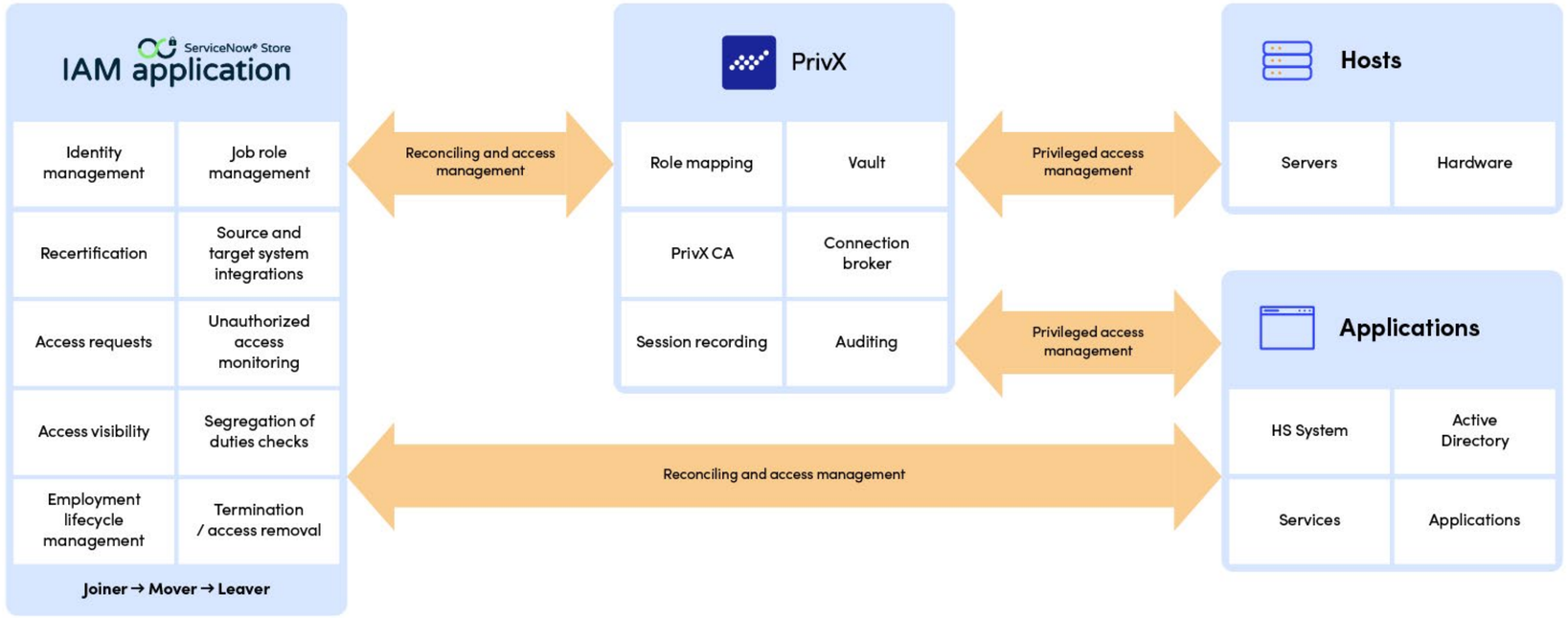
The combination of IAM and PAM helps organizations to centralize and unify identity-related and user access-related processes. At the same time, an IAM-PAM solution becomes the single point of control over these processes which simplifies the overall identity, access, and account management.

How does it work?

We at SSH together with our partner Appmore created a combined IAM-PAM solution that helps organizations manage identities, access, roles, and approval workflows. The solution unifies daily processes, like the joiner-mover-leaver process or access revocation, and simplifies monitoring and auditing to ensure smooth operations and regulatory compliance.

In a nutshell, we created a powerful platform that combines:

- IAM's authentication (MFA, SSO, etc.) and entitlements
- PAM's role-based access control (RBAC), access monitoring, session recording, and auditing
- Ticketing and approval workflows with native integration to the ServiceNow app



How does it work: 4-steps process

1. Access requests and granting

Users can request access via Appmore's ServiceNow application, and admins can easily grant access based on roles.

The application eliminates the need for email or other legacy solutions for handling access requests. HR can integrate their joiners, movers and leavers process with identity and (privileged) access management.

2. Passwordless authentication

When possible, users can utilize passwordless authentication methods, like biometric authentication. When needed, credentials like passwords and keys can be still used, vaulted, rotated, and managed appropriately.

3. Access monitoring and compliance

The solution provides the necessary tools to comply with access requirements of regulations such as GDPR, ISO27K1, and PCI DSS.

Access is automatically revoked when anomalies occur during a session, for example, if the antivirus solution is disabled.

4. Automatic access revocation

When an employee's tenure ends, the IAM application manages the inactivation of users' accounts and the removal of all access rights. Since PAM is synced with IAM, all access privileges are revoked at the same time.

Additionally, all actions, such as request, add, grant, and remove, are traced, and logged.

IAM module: ServiceNow by Appmore

The ServiceNow application streamlines IAM and IGA (Identity Governance and Administration) processes. By incorporating a governance and administration layer for all identities and access, this application enhances your overall IAM.

One of the key benefits of the application is its automation capabilities, which significantly reduce operational costs and increase efficiency. From access right ordering to approval, creation, and removal, the application streamlines the entire identity and access process lifecycle.

In addition, the IAM application provides you with the necessary tools to comply with access requirements for GDPR, ISO27K1, and PCI DSS. Its user-friendly interface and robust reporting capabilities offer complete visibility into all user accounts and accesses in the target systems, along with information on who ordered and approved them. The application enables access review of accounts and access rights, along with segregation of duties checks to help you pass internal or external audits.

With the application, users can easily request all access rights from ServiceNow's service portal. The application eliminates the need for email or other legacy solutions for handling access requests. Users and managers can order indefinite or temporary roles and remove unnecessary access when it is no longer needed.

When an employee's tenure ends, the IAM application manages the inactivation of their accounts and removal of all access rights, which greatly improves security. Additionally, the application allows you to deactivate a user's account during long leaves and reactivate it when the user returns, further enhancing security.

In summary, the IAM application for ServiceNow is a powerful solution for enhancing access and identity management, improving security, and streamlining compliance with regulatory requirements.

PAM module: PrivX by SSH

PrivX is a scalable, cost-efficient, and highly automated hybrid PAM solution that supports hybrid and multi-cloud environments. The solution increases security and operational efficiency by providing centralized access to mission-critical targets for superusers and privileged users without any credentials left behind. With PrivX, access to on-prem, hybrid, or cloud environments is managed centrally – all under one roof.

PrivX allows organizations to move to secure and cost-efficient passwordless authentication while supporting password vaulting and rotation when still needed – allowing businesses to migrate at their own pace.

In the PrivX's Zero Trust model, connections are established using ephemeral certificates that are created just-in-time for a session and expire automatically shortly afterwards, leaving no credentials behind to manage, lose, share, or rotate.

Additionally, PrivX syncs with Active Directory and automatically maps existing identity groups. Users are then granted access based on their roles (role-based access control, RBAC), rather than identities. PrivX automatically grants just enough access to the right users, at the right time, for the right duration of time, and with the right level of privilege.

Benefits

Request and grant access based on roles
Role-based access control (RBAC) is enabled by SSH's PrivX PAM based on the roles automatically provisioned by Appmore's integrated IAM. Users can easily request access, which is then granted automatically based on their role's permissions. Admins can easily grant temporary or permanent access based on a task, project, etc.

Seamless workflow approvals
Utilize automatic support for the joiner-mover-leaver process, including third parties. When employees join, move, or leave projects within the organization as per HR processes, this approach ensures that access is granted, modified, or revoked as necessary.

Ensure compliance with regulatory requirements
All actions, such as request, add, grant, and remove, are traced and logged which makes recertification of user roles a natural part of the solution. This ensures that the privileged and other rights meet the roles granted to the specific user(s) and follow regulatory requirements.

Minimize the risk of unauthorized access
The solution automatically detects anomalies in sessions (e. g. PAM bypass) and reports them. In case of company policy violation, the solution automatically revokes access - even if users have otherwise valid credentials.

Fulfill the requirements for the Segregation of Duties (SoD)
This can prevent, for example, test-to-production access or payment and approval of an invoice being granted to the same person. This is a fundamental requirement for many regulatory standards and processes, such as PCI DSS.

Enable end-to-end passwordless authentication
Grant passwordless access just-in-time for the session without users ever seeing or handling the secrets needed to establish the connection. Use methods like biometric authentication and single sign-on (SSO) to build a passwordless path for your users. It's convenient, secure, and efficient.

Background

About 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

About Appmore

Appmore provides and manages business applications with a mission to deliver maximum value to customers. Customer satisfaction is key, and everyone at Appmore works diligently to meet customers' true needs in an agile and responsive manner.

The commitment to exceptional customer service is rooted in Appmore's focus on meeting the unique needs of each individual customer. The goal is to provide a seamless experience that is tailored to customers' specific business requirements.

With well over a decade of experience serving customers, Appmore have completed hundreds of projects related to ServiceNow and Identity and Access Management and have consistently earned high marks for customer and employee satisfaction.

appmore.com

Helsinki
Global and EMEA headquarters
SSH Communications Security Corp.
Karvaamokuja 2B, Suite 600
FI-00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

New York City
AMER headquarters
SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel. +1 781 247 2100
info.us@ssh.com

Singapore
APAC headquarters
SSH CommSec Pte. Ltd.
24 Sin Ming Lane, #03-99 Midview City
Singapore 573970
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com