KEEPER PAM

Achieve visibility, security, access control and compliance across your entire organization.

Organizations today face escalating risks from compromised credentials, standing privileges, insider threats and overly complex PAM platforms. With cyberattacks targeting privileged accounts at all times, securing critical resources is a top priority.

To combat this, organizations often have multiple legacy solutions that are expensive and difficult to deploy and integrate. They do not monitor and protect every user on every device from every location. A streamlined, zero-trust approach to managing privileged access is essential to reducing attack surfaces, enforcing least privilege and ensuring regulatory compliance. This enables secure and efficient access for distributed teams across hybrid and multi-cloud environments.

Today's modern infrastructure requires a modern PAM solution

KeeperPAM secures and manages access to your critical resources, including servers, web apps, databases and workloads. Every user and device in your enterprise is authorized and authenticated with monitoring, threat tracking and reporting.

As a patented cloud-native, zero-knowledge platform, KeeperPAM combines enterprise password management, secrets management, connection management, zero-trust network access and remote browser isolation in one easy-to-use interface.

Benefits of KeeperPAM

Meet compliance requirements

Gain complete visibility with detailed logs, session recording and automated reports to ensure you have instant access to any data needed for audits.

Enable multi-cloud management

Centralize access in a single UI across multiple cloud providers, on-premises workloads and client environments.

Enforce MFA protection on every system

Add an MFA layer to cloud and on-prem infrastructure, including resources that do not natively support it.

Automate password rotation

Lock down service accounts across on-prem and cloud infrastructure.

Securely access every resource and account

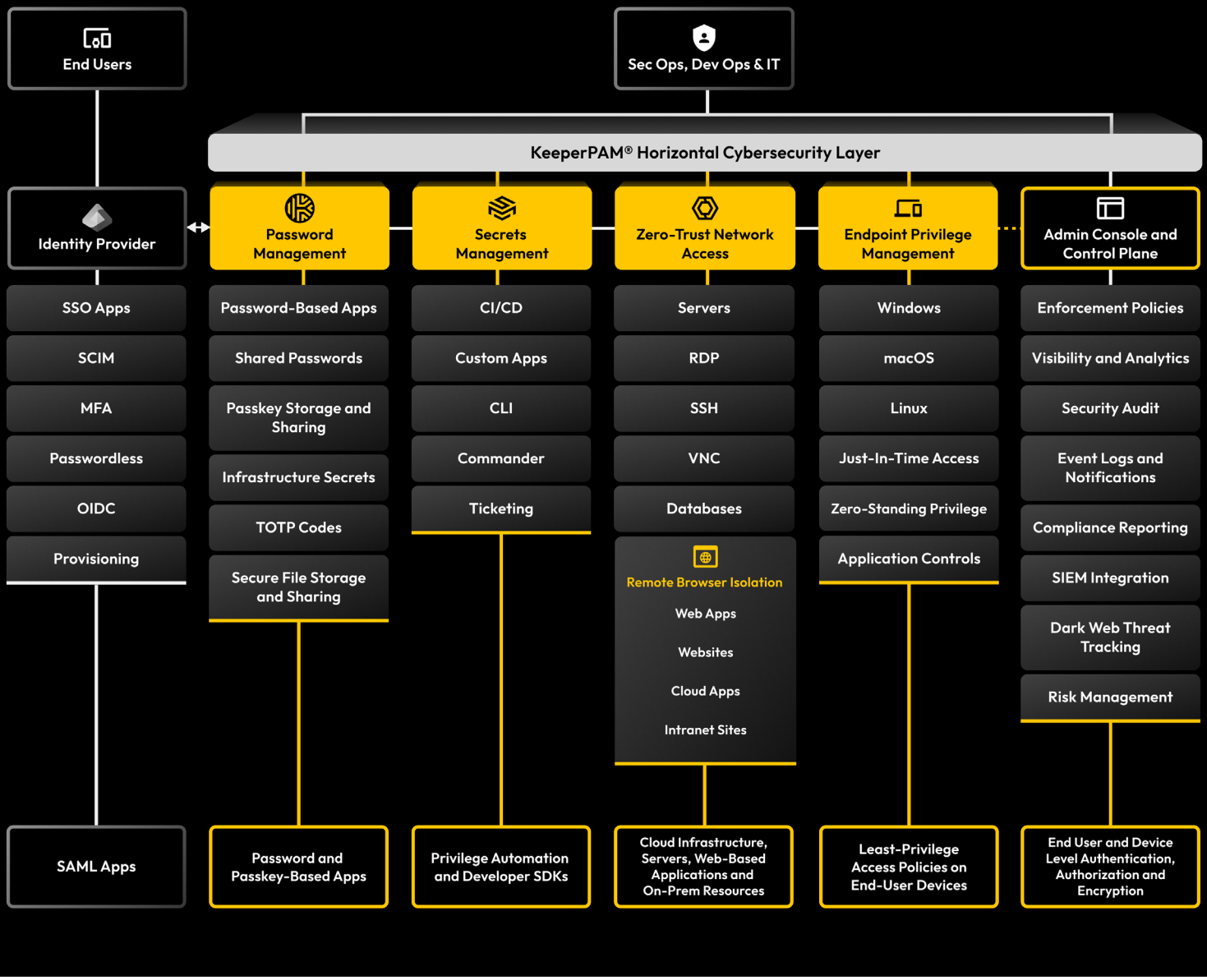
The Keeper Vault protects all users in the organization for complete coverage. Access is provisioned through policy, and KeeperPAM integrates with all IdPs and network infrastructure.

About Keeper Security

Keeper Security is transforming cybersecurity for people and organizations globally. Keeper's intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging.

KEEPER PAM

Keeper Privileged Access Management Platform



A next-gen PAM platform created for multi-cloud and distributed remote work environments

KeeperPAM is the first-ever solution to bring critical PAM functionality into a cloud vault that provides secure access to any protected resource. The platform enables organizations to achieve zero trust and eliminate standing privileges for all employees.

The platform can be fully customized to fit your organization's needs, such as configuring provisioning methods, enforcing granular access policies by role or team and integrating with hundreds of other IAM platforms like your SIEM, CI/CD, DevOps tools and custom software.

How to roll out KeeperPAM

1. **Deploy to users -** Deploy Keeper with your SSO, such as Entra ID or Okta, or through bulk user import. Provision through SCIM, SAML or AD.
2. **Set policy** - Apply MFA and role policies based on job responsibility and privilege in the Admin Console.
3. **Deploy the gateways** - Install a Keeper Gateway container in your target environments (e.g. AWS, Azure, on-prem). No network changes or ingress required.
4. **Discover and connect** - Manage access to resources such as machines, databases, web apps and service accounts in the Vault.