KEEPER®

The Modern PAM Platform

Keeper’s Mission

We prevent data breaches and mitigate cyber threats.

- Experts in Identity and Access Management (IAM), zero-trust and zero-knowledge security
- Industry pioneers with several U.S. patents covering IAM and zero knowledge
- Industry certifications including FedRAMP and StateRAMP Authorization, SOC 2 and ISO (27001, 27017 and 27018)
- Highest industry awards and user reviews
- Global AWS infrastructure for public and private sector cloud covering U.S., Canada, Europe, Japan and Australia
- Published in 21 languages with 120+ countries served

On average, more than 800 organizations per month purchase Keeper's cybersecurity platform which monitors and protects millions of employees and contractors on their devices and networks.

The Problem

Traditional layered cybersecurity solutions don’t stop data breaches

01

Most organizations have **inadequate visibility, security, control, compliance and reporting** capabilities over their users’ passwords, credentials and secrets on every device, application and system.

02

Organizations traditionally use a layered cybersecurity defense model, consisting of **disparate software products, that creates critical security gaps and vulnerabilities**.

KEEPER PAM®

The Solution

KeeperPAM
Zero-Trust Cybersecurity Platform

01

Secures and manages access to your critical resources, including servers, web apps, databases and workloads.

02

Unifies disparate IAM solutions into one ubiquitous platform with zero-trust and zero-knowledge security.

03

Enables organizations to achieve visibility, security, control and reporting across every user on every device.

KeeperPAM seamlessly integrates into existing tech and IdP stacks.

01

Deploy the Vault

Deploy Keeper with your SSO, such as Entra ID or Okta. Provision through SCIM, SAML or AD.

02

Set Policy

Apply MFA and role policies based on job responsibility and privilege.

03

Deploy the Gateway

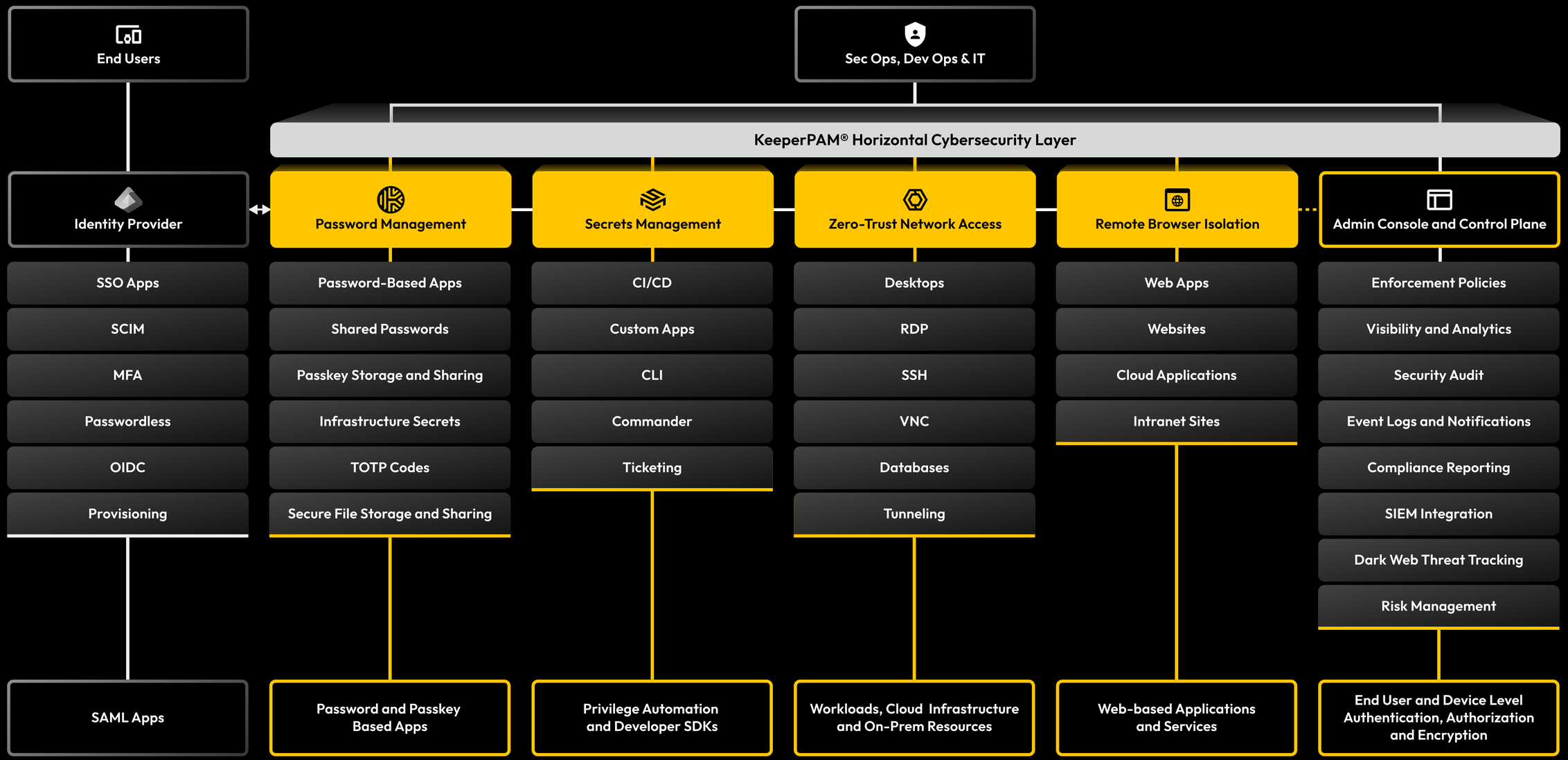
Install a Keeper Gateway in the target environments.

04

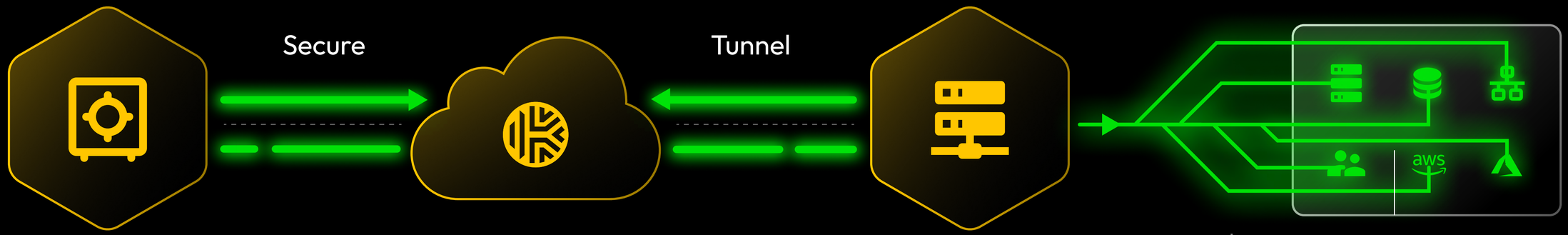
Discover and Connect

Manage access to resources such as machines, databases, web apps and service accounts.

Zero-Trust KeeperPAM Platform



Modern Architecture with Advanced Deployment Capabilities



Keeper Vault

User authenticates into the Keeper Vault applications

Keeper Cloud

Outbound-only, encrypted connections from Vault and Gateway

Keeper Gateway

Infrastructure

Infrastructure is managed through native protocols and Cloud APIs

KeeperPAM Addresses Pervasive Use Cases

- Password Mangement
- Password Sharing
- Password Rotation
- Secrets Management for DevOps
- Privileged Session Management
- Remote Infrastructure Access
- Zero-Trust & Zero-Knowledge

- Password Discovery
- Single Sign-On Security
- Passwordless Authentication
- Credential Governance & Controls
- SSH Key Management
- Secure Remote Database Access
- Industry Compliance & Reporting

Benefits of KeeperPAM

Securely access every resource and account

Meet compliance requirements

Enable multi-cloud management

Passwordless protection on every resource

Automate password rotation to lock down accounts

The Evolution of PAM Solutions

CYBERARK®

First PAM in the market

BeyondTrust

PAM with additional features

Delinea

(Formerly Thycotic)

PAM that disrupted market by being more affordable and easier to use

KEEPER PAM®

Industry’s first unified, next-gen PAM solution for perimeterless and multi-cloud IT environments

KeeperPAM Eclipses Legacy PAM Solutions

Legacy PAM products are ugly, difficult to deploy, difficult to use and do not protect every user on every device against modern adversaries.

Zero-Trust KeeperPAM

Cost Effective

Fewer products to purchase and easier for IT to manage with full organizational coverage

Fast Provisioning

Seamlessly deploys and integrates with any tech or identity stack

Easy to Use

Unified admin console and modern UI for every employee on all device types

Pervasive Visibility

Simplifies auditing and compliance with organization-wide role-based access control, event logging and reporting

World-Class Security

Keeper enables zero-trust transformation and is zero knowledge, which relegates all encryption key management at the client

Legacy PAM Solutions

Cost Prohibitive

Far more expensive product costs, maintenance and support

Difficult to Provision

Technically complex to deploy, requires dedicated resources with prohibitive or at-risk dependencies

Difficult to Use

Antiquated UI and product architectures that create end-user complexity and confusion

Opaque Visibility

Hindered by disparate, antiquated products that expose critical security and operational gaps which fail to terminate the kill chain

Inadequate Security

Legacy solutions are often not zero-trust or zero knowledge, and thus, cannot protect against modern threat vectors or adversaries

Core Capabilities of KeeperPAM

Password management

Protect and securely share passwords, passkeys and confidential data in a zero-knowledge vault with role-based access control, auditing and reporting.

Secrets management

Integrate CI/CD pipelines, DevOps tools, custom software and multi-cloud environments into a fully-managed, zero-knowledge platform and eliminate secrets sprawl.

Session management

Establish cloud and on-prem privileged sessions, create tunnels, enable zero-trust network access and provide secure remote database access without a VPN.

Remote browser isolation

Protects web-based apps, cloud apps and BYOD devices, prevents data exfiltration and controls browsing sessions with auditing, recording and credential autofill.

Admin console

Manages and deploys Keeper to users, integrates with identity providers, monitors activity and establishes role-based enforcement policies.

Control plane

Orchestrates and monitors the various components and activities related to privileged access, session management, policies and workflow.

Durable Competitive Advantage

01

Most robust security model and infrastructure in the industry with the largest number of certifications and authorizations for the mid-market, enterprise, for Federal and SLED segments - **the only FedRAMP and StateRAMP Authorized platform of its kind**, in the market.

02

The only platform in the IAM market that unifies enterprise password management, secrets management, zero-trust network access, remote browser isolation, threat tracking and reporting for enterprise-wide coverage.

03

Designed with zero-trust and zero-knowledge security from the ground up, across all client applications, to cover multi-cloud and distributed remote work environments.

Industry Leading Certifications and Authorizations

ISO 27001, 27017 and 27018

SOC 2

FedRAMP

StateRAMP

HIPAA

GDPR

FDA 21 CFR Part 11 Compliant

Level 1

EU-US Privacy Shield

PCI DSS Level 1

TRUSTe

FIPS 140-3

Thank You