Protect your users

Product Capability Briefing

George Kouimintzis
Commercial Director, NSS

Affordable Cutting Edge

December 6, 2023

About Keeper Security

- Founded in 2011
- Experts in Identity and Access Management (IAM)
  - Enterprise Password Management
  - Secrets Management
  - Privileged Access Management (PAM)
- 2.5M paying customers, including 1.5M B2B (YE 2022)
- Published in 21 languages
- Profitable and funded by Insight Partners
  - ~ USD $30B in capital commitments
- Holds several patents covering IAM, password security, 2FA, dark web protection and SSO integration
- Highest-ranked in industry awards and user reviews
- Cloud data centers in the United States, Canada, Europe, Japan and Australia

Keeper protects millions of people and thousands of organizations globally as the trusted and proven cybersecurity leader.

Protects organizations, large and small.

App Store
Top-Rated Productivity
4.9 out of 5 stars

Google Play
Over 10 Million Installs
4.6 out of 5 stars

G2 Crowd
2021 Enterprise Leader
4.8 out of 5 stars

PCMag
Editor's Choice
4.5 out of 5 stars

Gartner peerinsights™
4.5 out of 5 stars

Trustpilot
4.4 out of 5 TrustScore

GetApp
4.7 out of 5 stars

spiceworks
4.9 out of 5 stars

nss
Affordable Cutting Edge

KEEPER®

Leading organizations use Keeper’s cybersecurity platform.

NIS 2 Directive

- NIS 2 stands for “Network and Information Security Directive” and is a continuation and expansion of the previous EU cybersecurity directive, NIS 1
- NIS 2 greatly expands which organization are impacted by its requirements and is careful to distinguish between “essential companies” and “important companies”
- Deadline : 18 October 2024 for the member states

nss
Affordable Cutting Edge

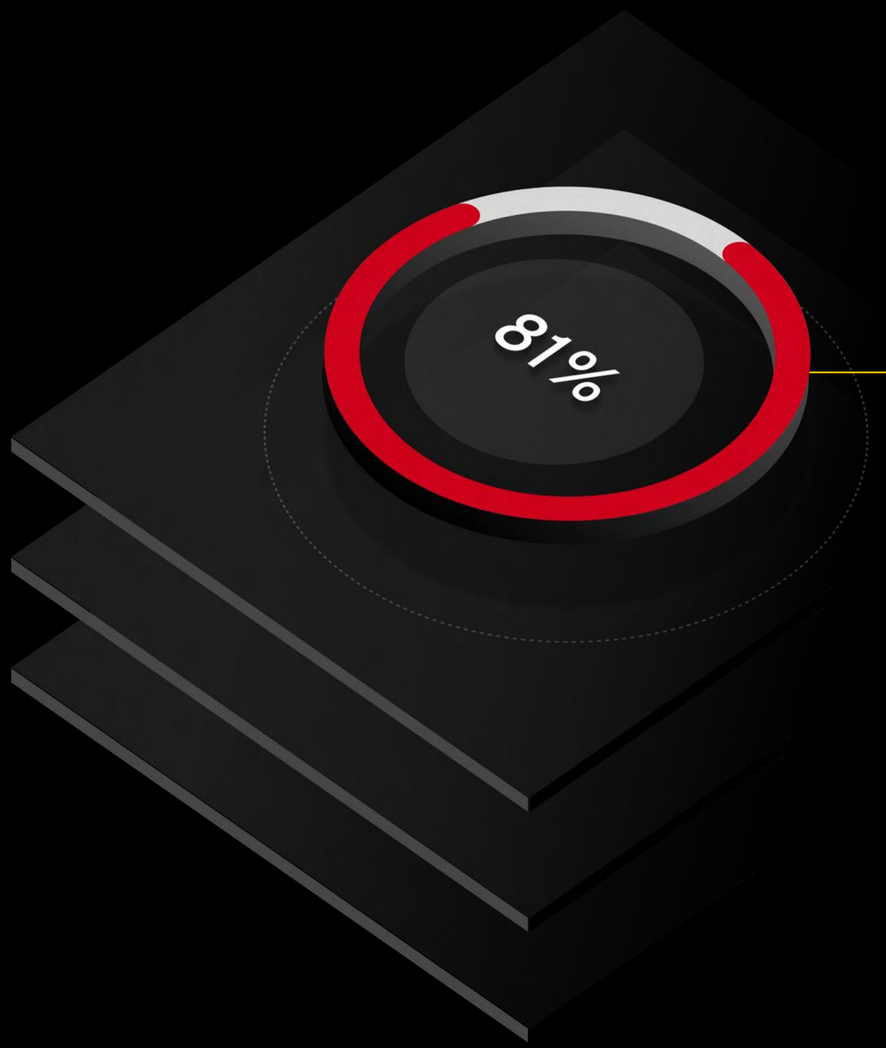
KEEPER®

NIS 2 proposed solutions : **Keeper**

- business continuity, and crisis management
- security in network and information systems
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- policies and procedures regarding the use of cryptography
- human resources security, access control policies and asset management

nss
Affordable Cutting Edge

KEEPER®



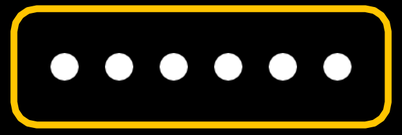
81% of breaches are due to a failure to secure passwords, credentials and secrets*

*Verizon Data Breach Report 2022

Protecting passwords, credentials and secrets, is now the world's most pervasive cybersecurity issue.

Problem 1

No visibility, security or control over employee passwords, credentials and secrets



Stolen and weak passwords and secrets are the leading cause of data breaches – yet most organizations have no visibility, security or control over their users' passwords, credentials and secrets on every device, application and system.

This creates existential insider and external threat risks.

Problem 2

Failure to protect every user on every application
on every device from every location

Every person in an organization is susceptible to a credential-related attack which could result in a security breach.

Every second that passes without protecting every user on every device puts the organization at risk.

Problem 3

The security-adoption paradox

The more secure the solution, the fewer employees want to use it.
The less they use it, the less secure their organization is.

Key Internal and External Challenges for Organizations

1. An organization's **infrastructure consists of both humans and machines** which need to be protected.
2. The **traditional IT perimeter has vaporized** due to distributed remote work and multi-cloud computing.
3. The **attack surface has exponentially increased** with more sophisticated attacks on additional devices, credentials and secrets on remote networks.
4. **Traditional cybersecurity solutions are heterogeneous**. Disparate, isolated software products provide inadequate visibility, security, reporting and control.
5. **Heterogeneous IT environments radically increase operating risk** because they create critical security gaps which leave organizations vulnerable.
6. **Purchasing, deploying and managing disparate software is cost-prohibitive** and does not protect against modern internal and external threats.

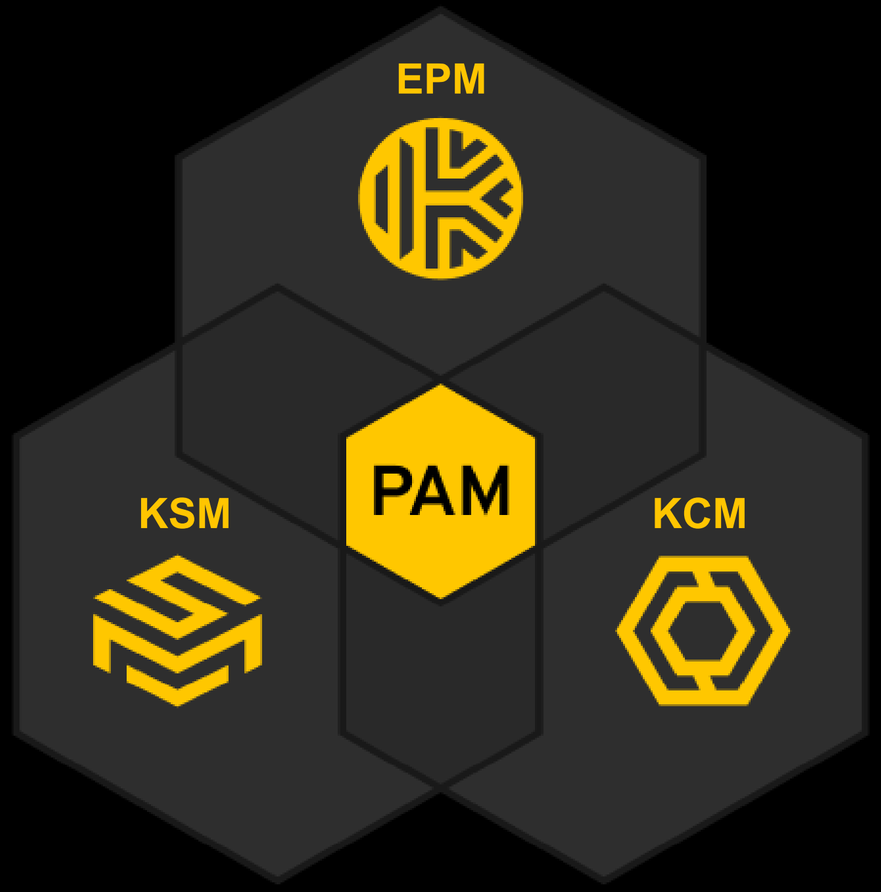
The Solution: A Unified Next-Gen PAM Platform

Keeper's cybersecurity PAM SaaS-based platform enables organizations to achieve full visibility, security, control and reporting across every user on every device in an organization.

The platform enables **zero-trust and zero-knowledge** security and compliance by unifying three integral products into one platform.

The Next-Gen, SaaS-Based, Unified Zero-Trust PAM

The first company in the industry to unify three essential IAM products
for unparalleled cost-effectiveness, rapid provisioning and ease-of-use.



Keeper Enterprise Password Manager (EPM)
Enables organizations to manage, protect, discover, share and rotate passwords with security, control and visibility to simplify auditing and compliance.

Keeper Secrets Manager (KSM)
Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

Keeper Connection Manager (KCM)
Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access -- without the need for a VPN with RDP, SSH keys, database, and Kubernetes.

nss
Affordable Cutting Edge

KEEPER®

Keeper PAM Eclipses Traditional PAM Solutions

Traditional PAM products are ugly, expensive, difficult to deploy, difficult to use and do not monitor and protect every user on every device from every location.

Keeper PAM Platform

- **Cost Effective.** Fewer products to purchase and easier for IT to manage with fewer people.
- **Fast Provisioning.** Seamlessly deploys and integrates with any tech or identity stack – in a few hours.
- **Easy to Use.** Unified admin console and modern UI for every employee on all device types – average training is less than 2 hours.
- **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.

Traditional PAM Solutions

- **Cost Prohibitive.** Far more expensive product costs, maintenance and support.
- **Difficult to Provision.** Technically complex to deploy, requires dedicated resources having an average deployment time of 6 to 18 months.
- **Difficult to Use**. Antiquated UI and product manuals that are often > 1,000 pages create end-user complexity and confusion.
- **Opaque Visibility.** Hindered by disparate, antiquated products that focus on IT staff – not the entire organization.
- **Inadequate Security.** Traditional solutions are often not zero-trust or zero knowledge and thus, cannot protect against modern threat vectors.

Keeper PAM Addresses the Key Pain Points and Requirements in Organizations to Prevent Data Breaches

- Password Management
- Password Sharing
- Password Rotation
- Secrets Management for DevOps
- Privileged Session Management
- Remote Infrastructure Access
- Zero-Trust, Zero-Knowledge Security
- Password Discovery
- Single Sign-On Security
- Passwordless Authentication
- Credential Governance & Controls
- SSH Key Management
- Secure Remote Database Access
- Industry Compliance & Reporting

NSS Affordable Cutting Edge

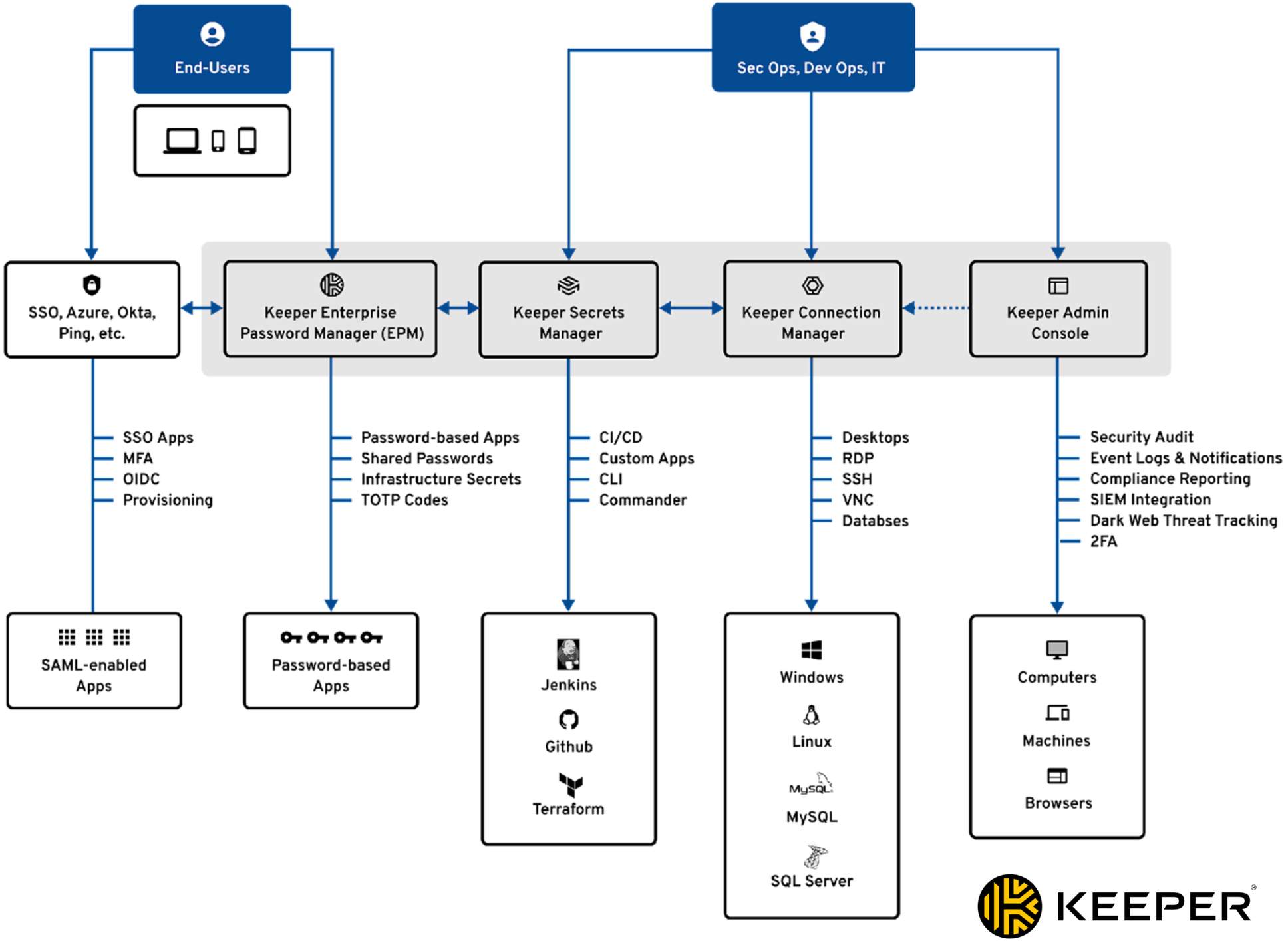
KEEPER®

Zero-Trust Framework and Zero-Knowledge Security Architecture

1. Data is encrypted and decrypted at the device level (not on the server)
2. The application never stores plain text (human-readable) data
3. The server never receives data in plain text
4. Keeper employees and 3rd parties can never view unencrypted data
5. The keys to decrypt and encrypt data are derived from the user's master password
6. 6. Multi-layer encryption provides access control at the user, group and admin level
7. Sharing of data uses Public Key Cryptography for secure key distribution

Visit https://keepersecurity.com/security.html

Keeper's Zero-Trust PAM Platform seamlessly integrates into any existing identity stack and infrastructure.



Affordable Cutting Edge

KEEPER

Keeper Security Certifications

ISO 27001

SOC 2

FedRAMP

StateRAMP

HIPAA

GDPR

PCI DSS Level 1

TRUSTe

Level 1

FIPS-140-2

EU-US Privacy Shield

nss
Affordable Cutting Edge

KEEPER®

Visit us at the Expo area.

Thank you.

KEEPER®

nss

Affordable Cutting Edge