KEEPER® | **VAYNERX**

Case Study

VaynerX Deploys Keeper Enterprise-Wide Across a Global Workforce

Background

VaynerX is a global modern media and communications company, founded by Gary Vaynerchuk, that operates at the intersection of brand, culture and technology. Headquartered in New York City, VaynerX is the umbrella organization for a portfolio of companies that includes VaynerMedia and several other specialized entities. Collectively, these businesses support some of the world's most recognizable brands across advertising, commerce, media, influencer marketing and digital transformation.

Industry
Advertising and Communications

Employees
2,000+

Solutions
Enterprise Password Manager
- Advanced Reporting & Alerts Module (ARAM)
- Platinum Support

The Challenge

Prior to adopting Keeper, the organization's credential management was decentralized. VaynerX wanted the best solution to streamline daily operations and strengthen its security posture when managing clients' accounts. Internal teams routinely access client-owned systems, making credential security essential to protecting not only internal operations but also client trust and long-term partnerships.

> "Prior to Keeper, we weren't using a unified approach across the organization that could capture everything in a single pane of glass."
>
> John Georgatos | Global Chief Information Officer, VaynerX

The Keeper Solution

To address these challenges, VaynerX conducted a formal evaluation of enterprise password management platforms and ultimately selected Keeper. The decision was driven by Keeper's security architecture, administrative depth and its ability to scale across a complex, multi-entity organization without disrupting productivity.

> "Choosing Keeper came down to its functionality, ease of use and the ability to centrally manage the system, giving us enterprise-level security access."
>
> John Maalouf | SVP, Global Head of Procurement, VaynerX

Centralized Credential Management - Built on a **zero-trust, zero-knowledge architecture**, Keeper provided VaynerX with a centralized platform to securely manage credentials while maintaining enterprise-grade governance and control. Keeper was deployed as the standard password management solution across all VaynerX entities, supporting both centralized governance and local team collaboration. From the outset, the goal was not simply to introduce a password vault, but to establish a secure, enterprise-wide system for credential lifecycle management.

> "What ultimately led us to Keeper was how simple it was to integrate with our existing identity provider, Okta, and how well both platforms coexist with each other."
>
> **John Georgatos | Global Chief Information Officer, VaynerX**

Seamless Integration with Existing Infrastructure - Keeper integrated seamlessly with Okta to support **Single Sign-On (SSO)**, automated user provisioning and deprovisioning, creating a simple and easy authentication experience. Employees gain access to Keeper as part of their normal login flow, while IT maintains centralized control. Through Google Workspace, administrators also deployed the **KeeperFill®** browser extension organization-wide, accelerating adoption and enabling secure autofill across websites and applications.

> "Keeper impressed me with the native nature of the Google Chrome extension. Keeper automatically fills the password field, and you don't have to leave the website that you're trying to log into."
>
> **John Maalouf | SVP, Global Head of Procurement, VaynerX**

User Adoption and Training Support - Keeper provides extensive **product documentation**, implementation resources and customer success support to guide organizations through enterprise-wide deployment. At VaynerX, these resources were paired with internal communications and live training sessions to support a smooth rollout across a global workforce. Keeper is recognized as the leading password manager for organizations of all sizes and is easy to use and quick to deploy. For end users, detailed **product guides** and **training videos** drive high user adoption.

> "Leading up to launch, Keeper's Customer Success Team was right there with us to walk us through every single training and make sure that our adoption rate was getting to the point that we wanted it to."
>
> **John Georgatos | Global Chief Information Officer, VaynerX**

Cost-Effective - No matter the size or type of organization, Keeper has a cost-effective plan to fit and scale with organizational needs. Keeper's transparent pricing model, paired with world-class customer support, ensures that organizations maximize their investment.

Best-in-Class Security - Keeper's zero-trust, zero-knowledge security architecture is unmatched at safeguarding information and mitigating the risk of a data breach. Keeper combines device-level, Elliptic Curve Cryptography (ECC) with **multiple layers of encryption** (at the vault, folder and record levels), multi-factor and biometric authentication. Keeper is **SOC 2 and ISO 27001 compliant** — with the longest-standing compliance in the industry — as well as FedRAMP High and GovRAMP Authorized.
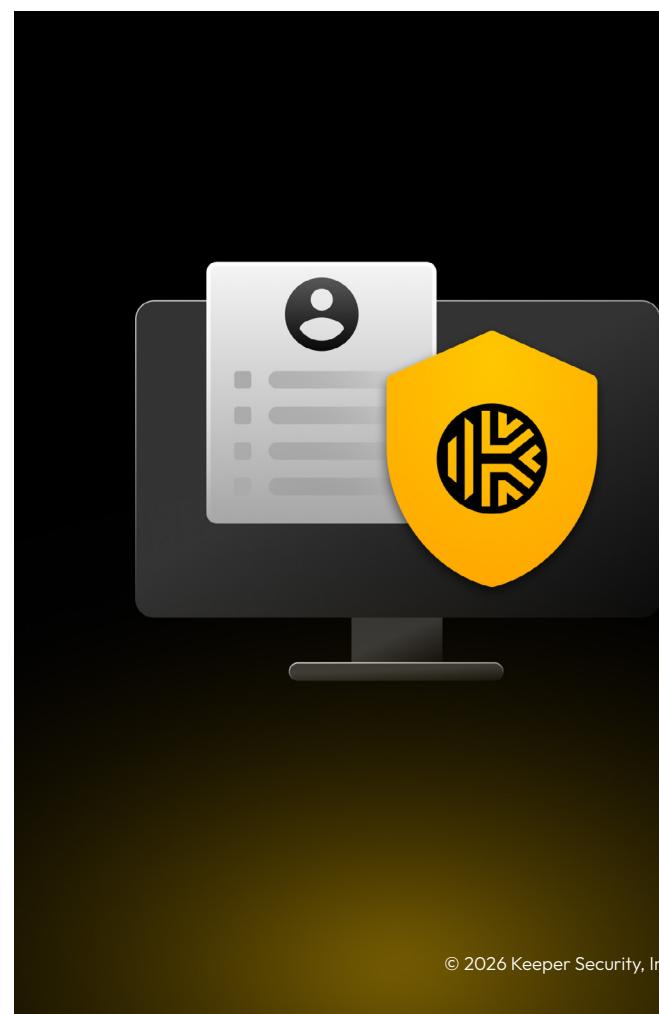
KEEPER®

Organization Impact

The deployment of Keeper had a broad and lasting impact across VaynerX, strengthening overall security, improving operational efficiency and reinforcing a culture of shared responsibility for protecting critical data.

Stronger Security Posture and Centralized Governance - With Keeper deployed enterprise-wide, VaynerX gained consistent visibility into how credentials are created, stored, shared and accessed. Security teams can now enforce password standards, reduce reuse and proactively manage risk across internal systems and client environments. This approach reduced risk not only for internal systems but also for client-owned platforms that VaynerX teams access daily.

> "Everyone here uses Keeper. It is not an option, and we like it that way."
>
> **Christine Kadets | Director of Procurement, VaynerX**

Improved Operational Efficiency for IT and Security Teams - Keeper streamlined onboarding and offboarding processes by enabling secure credential transfers and centralized access management. As a result, VaynerX experienced a noticeable reduction in password-related IT support requests.

Secure, Scalable Client Collaboration - Client work is core to VaynerX's business, and Keeper's easy-to-use sharing capabilities directly support that model. Keeper's **bidirectional One-Time Share** feature enables VaynerX to receive sensitive credentials from clients and vendors outside the organization without relying on email or shared documents, even if they are not Keeper users.

> "The bidirectional One-Time Share feature has been incredibly helpful and, more importantly, helps us securely share information between our clients and vendors."
>
> **John Georgatos | Global Chief Information Officer, VaynerX**

High User Adoption and Minimal Disruption - Keeper's ease of use, browser extension and mobile accessibility drove strong adoption across technical and non-technical teams alike. VaynerX successfully onboarded 99.5% of its employees within the Keeper platform. Keeper is now a pivotal tool in daily workflows for storing, managing and generating secure credentials, and has been transformative for the organization.

Positive Impact Beyond the Workplace - Keeper's availability for personal use, with a free Family Plan provided to employees, reinforced strong security habits beyond VaynerX, helping employees apply the same best practices in their daily lives. By extending secure credential management outside of work, the organization further reduced risk while fostering a culture of security awareness.

> "Keeper helps us to achieve the transformation goals of our organization, which are centralization, consolidation and standardization."
>
> **John Georgatos | Global Chief Information Officer, VaynerX**

Overall, Keeper has become a core component of VaynerX's cybersecurity strategy, supporting secure password and passkey usage, reinforcing client confidence, providing unparalleled visibility and enabling teams to focus on delivering impact at scale without slowing down business operations.

Keeper Password Manager

Most businesses have limited visibility into employees' password practices, which can significantly increase cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance. Keeper solves this by providing ultimate security, visibility and control.

Data is protected with Keeper's zero-knowledge security architecture and world-class encryption. Zero-knowledge means only the user knows and has access to their master password and the encryption key used to encrypt and decrypt their information.

Keeper is intuitive and easy to deploy, regardless of business size. Keeper integrates with Active Directory and LDAP servers, which streamlines provisioning and onboarding. **Keeper SSO Connect**® integrates into existing SSO solutions and is FedRAMP High and GovRAMP Authorized.

Keeper is designed to scale for organizations of any size. Features such as role-based permissions, team sharing, departmental auditing and delegated administration support organizations as they grow. **Keeper Commander** provides robust APIs for integration with current and future systems.

Business Use Cases: Keeper Password Manager

- Prevent password-related data breaches and cyber attacks
- Support passkeys for effortless authentication
- Strengthen compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimize training with fast time-to-security
- Improve employee security awareness and behavior

About Keeper

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organizations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognized for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organizations to defend against modern cyber threats at **KeeperSecurity.com.**

Keeper is trusted and loved by thousands of companies and millions of people globally.

G2
Enterprise Leader

PCMag
Editor's Choice

App Store
Top-Rated Productivity

Google Play
Over 10 Million Installs