1Password

1Password for Saudi Arabian businesses

Use cases, security architecture, and regulatory alignment

Author: Andrew J. Grotto

Version: 1.0

Published: June 1, 2026

Executive summary

This document assists stakeholders in the software purchasing process in the Kingdom of Saudi Arabia who are considering 1Password to secure credentials for their organization.

It outlines:

- The use cases for enterprise password managers, especially in increasingly AI-driven environments
- Why analysts and regulators around the world recommend password managers to centrally manage and protect credentials
- 1Password's unique security architecture, which ensures that ownership of and access to stored credentials belong exclusively to the account holder
- The Kingdom of Saudi Arabia's regulatory environment, and how it aligns with 1Password

While businesses should consult with their legal counsel before adopting any new tooling, this document describes how 1Password's zero-knowledge architecture advances the security and resilience goals of Saudi Arabia's policy and regulatory frameworks for cybersecurity and digital sovereignty.

Introduction

Digital credentials are the gatekeepers of digital identity, facilitating trillions of dollars in e-commerce, banking, and data exchange. Credential-related security failures, however, are among the leading causes of cyber incidents: abused credentials have been the top or second-most initial access vector for several years running, according to IBM X-Force. They were present in nearly one-third of cases in 2025.[1]

Using strong, unique credentials for each digital service and keeping them safe is therefore one of the most effective ways to reduce cyber risk. This is virtually impossible for humans to do without help, however, because it requires memorizing dozens, even hundreds of complex credentials and keeping them updated.

The problem of "credential sprawl" is also taking on a new urgency, thanks to the advent of automation and agentic AI. For many enterprises, the number of machine, human, and AI credentials already exceeds the number of employees.[2]

[1] IBM X-Force, "X-Force threat intelligence index 2026: Top initial access vectors," IBM, February 2026

[2] Andy Parsons, "96 machines per human: The financial sector's agentic AI identity crisis," CyberArk, October 14, 2025

Developers and emerging “AI builders” are creating new identities like API keys, tokens, service accounts, and database credentials. On top of that, browser-use agents still need usernames and passwords to navigate the web on the user’s behalf. Privileged Access Management (PAM) is complex to implement and doesn't solve the general problem of easily and securely brokering credentials to these AI agents.

No matter the size of a business, credential sprawl is real and primed to grow as SaaS adoption accelerates, teams spin up their own “shadow AI” and other tools, and AI agents and vibe-coding tools become more prolific. Attackers will feast on this sprawl unless defenders implement solutions to get it under control.

Password managers: Recommended by regulators and researchers

Enterprises typically have complex identity security stacks, often with multiple, redundant IAM, SSO, and PAM tools, which can secure nearly any application that can be federated. These systems are often cumbersome, however, making it hard for IT and security teams to keep up with securing a growing roster of SaaS apps, shared accounts, and AI tools.

Regulators agree that password managers are a proven way to help.[3] An effective password manager prompts users to create complex and unique passwords for each digital service. Complex passwords are virtually impossible for hackers to guess using brute-force guessing algorithms, while unique passwords prevent hackers from using a single password to unlock multiple accounts. An effective password manager stores this password data in a digital vault accessible only by the legitimate user, without leaving copies in the end user’s device.

The security of these digital vaults is critical. Governments around the world are sounding the alarm about tech sovereignty, with data protection among the driving concerns. Regulators want to ensure that vendors providing digital services within their jurisdictions comply with data protection laws and cannot be compelled or coerced by foreign powers to violate those laws. The key tech sovereignty matter for vendors of password managers is whether a foreign power can force a vendor to share the credentials stored in its customers’ vaults.

A vendor’s exposure to this risk depends fundamentally on the architectural design choices it has made about its product – particularly, whether they hold the keys needed to decrypt customers’ data. 1Password’s customers’ password data is encrypted and decrypted on their local device using keys derived from secrets that 1Password does not know and cannot discover. The customer, not 1Password, is in sole possession of the key needed to decrypt the encrypted passwords stored in the customer’s vault.

[3] European Union Agency for Cybersecurity (ENISA), “Cyber Hygiene”
“Managing Passwords with a Password Manager”
“Trusting the tech: using password managers and passkeys to help you stay secure online,” UK National Cyber Security Centre,

1Password's zero-knowledge architecture

1Password's architecture is based on a zero-knowledge security model that enables 1Password and its customers to make use of secrets – encryption keys – without revealing those secrets to each other.[4] 1Password hosts customers' password vaults, which contain encrypted versions of the customers' passwords. This data is encrypted using AES-256-GCM, the same encryption approved by the NSA to protect classified U.S. Government documents, using keys that 1Password never knows and cannot derive.

The keys that encrypt 1Password data are, in turn, encrypted by a user's Account Unlock Key (AUK). The AUK is derived from either a device key unique to each app the user signs into (when unlocking 1Password with SSO), or from the combination of a user's Account Password and Secret Key. In other words, the data stored by 1Password is worthless to an attacker unless the attacker can derive a customer's AUK, which 1Password does not know and cannot derive. This is due to 1Password's zero-knowledge end-to-end encryption model.

When a customer sets up their 1Password account, they must create and memorize an account password for unlocking the 1Password app (if they aren't using SSO to unlock 1Password). At the same time, 1Password uses the customer's endpoint device to generate a random 128-bit Secret Key. Neither the user's chosen Account Password nor the locally-generated Secret Key is ever transmitted to 1Password. They exist only locally on the user's device and in their head. When unlocking 1Password, these two secrets are combined to derive the user's Account Unlock Key, which can decrypt the keys required to authenticate with 1Password's servers and to locally decrypt data stored in 1Password.

As with any zero-knowledge system, 1Password strongly encourages customers to have a recovery process for the account password because 1Password's design decision also means it has no ability to recover or reset account passwords.

When using SSO, there is no Account Password and Secret Key. Instead, when the user creates an account, their browser stores a random 256 bit device key. Each 1Password app or browser a user signs into has its own unique, device-bound device key. Upon successful SSO authentication, 1Password releases that user's encrypted credentials bundle for the user's 1Password client or browser to decrypt with its device key.

Whether using the Account Password and Secret Key or SSO, an attacker cannot acquire the relevant key material or keys from 1Password. When accounts use an Account Password and Secret Key, 1Password uses a process called two-secret key derivation (2SKD) to derive the Account Unlock Key locally from secrets known only to the 1Password user or their device. With SSO, each browser or client's Device Key is never transmitted between client applications or to 1Password's servers and is never co-located with keys that decrypt your 1Password data.

[4] "1Password Security Design," See 1Password

In either case, all encryption and decryption happens locally on a user's device, using keys derived locally from secrets known only to the user or their device, and which 1Password never knows and cannot derive. All data is encrypted on device before ever being sent over the network to 1Password's hosting infrastructure.[5]

In addition, this encrypted data is further prepared for transmission between 1Password and customers with an additional secure in-transit protection that enables the encryption "handshake" that the encryption bundle enables instead of the weaker "authentication" method that most websites use. 1Password uses Secure Remote Password (SRP) for authentication as it connects to the 1Password local cache that is created on device to support the encryption process and provides a local backup to all the secret data that user has been permissioned to access. This is in addition to the server authentication provided by TLS. Not only does the client prove its identity to the server, but the server proves its identity to the client.

For organizations that use single sign-on (SSO), 1Password uses a similar underlying methodology to layer its zero-knowledge architecture onto SSO. On devices where a user signs in with SSO, 1Password clients store a device level key. Each device level key is uniquely and randomly generated, and never leaves the device on which it was created. To enroll a new device on an SSO-enabled account, the user must authenticate first, then authorize the new device using a previously enrolled device. Subsequently, when a user signs in with SSO, they sign in with the username, password, and other factors required by their SSO provider instead of using their account password and Secret Key to authenticate to 1Password. 1Password collaborates with the SSO provider to proof of authorization as authentication.

The combined use of a Secret Key and account password (or a locally-stored 256-bit Device Key in the case of SSO) means that an attacker who has acquired the customer's account password and the encrypted vault data still cannot decrypt the vault data. It also stymies an attacker in possession of the Secret Key and the encrypted vault data. The attacker would need all three pieces of information: the account password, generated and memorized/stored by the customer; the Secret Key, generated and stored locally on the customer's endpoint;[6] and the encrypted vault data hosted by 1Password – to read the customer's plaintext passwords managed by 1Password. SSO and the use of device keys provide similar protections, requiring an already-trusted 1Password application and complete SSO credentials before any decryption can happen. This encryption methodology makes stolen email and account password credentials useless on a device that doesn't have the Secret Key present. This makes signing in from an untrusted device practically impossible.

[5] While 1Password's two-secret system provides strong security, the platform also supports additional two-factor authentication (2FA) for account access. This is implemented through Time-based One-Time Passwords (TOTP) using authenticator apps or hardware security keys supporting FIDO U2F/WebAuthn. The 2FA integration demonstrates defense-in-depth: the Secret Key provides cryptographic security against server breaches, the Master Password provides user authentication, and 2FA provides an additional authentication factor against credential compromise.

[6] 1Password implements memory protection techniques to minimize exposure of sensitive data on endpoints. Plaintext passwords and cryptographic keys exist in memory only when necessary for active operations. Upon locking or application termination, sensitive memory regions are explicitly zeroed before deallocation. The applications use secure memory handling to prevent sensitive data from being swapped to disk. On platforms supporting it, memory pages containing keys and plaintext data are marked as non-swappable, preventing the operating system from writing them to page files or swap space.

Kingdom of Saudi Arabia: Strategic context

Saudi Arabia has elevated cyber resilience to a national security priority over the past decade, embedding cybersecurity in its Vision 2030 agenda and establishing the National Cybersecurity Authority (NCA) as central regulator, standard-setter, and coordinator for cybersecurity across the Kingdom, with both strategic and enforcement powers. It issued version 1 of the Essential Cybersecurity Controls (ECC) in 2018 and extended them with the Cloud Cybersecurity Controls (CCC) in 2020 and the Data Cybersecurity Controls (DCC) in 2022 (DCC-1:2022).[7] In December 2023, the NCA issued an expansive "Cybersecurity Toolkit" of regulations and policies "to enhance cyber readiness and reduce cyber risks" in Saudi Arabia,[8] followed by updated versions of the ECC and CCC in 2024 (ECC-2:2024 and CCC-2:2024).[9] Most recently, in December 2025 the NCS hosted a public consultation on updated National Cryptographic Standards (NCS-2:2025).

Adversarial targeting of Saudi critical infrastructure – especially in the energy sector – has been a recurring feature of its threat landscape, with destructive malware campaigns and intrusions against oil and gas entities underscoring the potential for cyber operations to produce physical and economic disruption. Attacks on government ministries, financial institutions, and media organizations have likewise highlighted the use of cyber tools for regional influence, coercion, and information operations.

Supply chain and third-party risks understandably shape Saudi threat perceptions, given the Kingdom's reliance on foreign technologies, managed services, and industrial control systems sourced from a diverse set of global vendors. This has driven a push for tighter controls on procurement, stricter requirements for local and foreign suppliers, and greater emphasis on data localization, secure cloud adoption, and vetting of telecoms and infrastructure providers that could become conduits for espionage or disruption.

The surge in criminal ransomware, data extortion, and financially motivated intrusions against Gulf entities has added another layer of urgency, exposing sensitive personal and commercial data and imposing tangible operational and reputational costs on Saudi organizations. In response, the Kingdom has expanded mandatory incident reporting, strengthened penalties and compliance expectations, and promoted wider adoption of baseline cyber controls across public and private sectors as it seeks to protect both legacy oil infrastructure and rapidly growing digital services, making user-friendly, cost-effective approaches to resilience an imperative.

At the same time, the Kingdom's Vision 2030 identifies digital sovereignty as a national priority, with AI emerging as a strategic focal point for the Kingdom's future security and economic prosperity. The Kingdom established the Saudi Data and AI Authority (SDAIA) in 2019 to drive AI and data innovation and governance. It is the primary data protection regulator under the Kingdom's Personal Data Protection Law and is also responsible for administering data localization mandates—a function transferred to it from the NCA in ECC-2:2024.

[7] National Cybersecurity Authority, "Data Cybersecurity Controls (DCC -1:2022)"

[8] National Cybersecurity Authority, "NCA has expands [sic] its Cybersecurity Toolkit" June 12, 2023

[9] National Cybersecurity Authority, "Essential Cybersecurity Controls (ECC – 2: 2024)"
National Cybersecurity Authority, "Cloud Cybersecurity Controls (CCC – 2: 2024)"

For enterprises in Saudi Arabia, this regulatory ecosystem requires looking beyond the hype and scrutinizing the actual performance and underlying architecture of vendors' products. For vendors of security solutions and their distributors, this means offering affordable products that help customers of varying size and cyber maturity build resilience while being transparent about how the technology complies with law and policy. For regulators, this means holding vendors to high standards of transparency and accountability about the security properties of their products and empowering customers to choose best-in-class solutions.

Regulatory context: Digital sovereignty and encryption

Encryption is a core tenet of the Kingdom's regulatory framework for cybersecurity, which also establishes stringent "key residency" requirements aimed at preventing sensitive key material from leaving Saudi Arabia. 1Password's zero-knowledge architecture puts customers, not 1Password, in control of their sensitive key material.

The ECC establishes baseline cryptography controls for enterprises and critical infrastructure, while the NCA's National Cryptographic Standards (NCS-1:2020) define the technical parameters of acceptable cryptographic standards. The CCC adapts and extends resources to establish encryption as a mandatory requirement for both Cloud Service Providers (CSPs) and their customers as part of its "Cybersecurity Defense" domain. 1Password is a CSP[10]. The DCC specifies data localization requirements, including for key residency.

Section 2-7 of CCC-2:2024 mandates that CSPs implement section 2-8-3 of ECC-2:2024, which requires "[e]ncryption of data in-transit and at-rest, as per their classification and the relevant legislative and regulatory requirements." Section 2-7 of CCC-2:2024 requires that CSPs implement "[t]echnical mechanisms and cryptographic primitives for strong encryption, in according to [sic] the advanced level in the National Cryptographic Standards (NCS-1:2020)." In practice, this means implementing AES-256 encryption for data at rest and TLS 1.2 or higher for data in transit: Section 2-1-2 of NCS-1:2020 lists AES-256 as satisfying the highest level of assurance ("Advanced"). As described earlier, 1Password uses AES-256 encryption for encrypting keys; its zero-knowledge architecture ensures that the encryption keys are encrypted on the user's device prior to transmission to 1Password servers. In addition, 1Password uses TLS and SRP together (stronger than TLS alone) for transmitting the AES-encrypted keys to and from its servers.

The CCC also addresses key management: both CSPs and CSTs must ensure well-defined ownership for cryptographic keys and keep an audit trail of keys. 1Password is transparent about its zero-trust architecture and has published detailed technical documentation.[11]

[10] CCC-2:2024 defines CSPs broadly as "Any natural or legal person (such as companies) who provides cloud computing services to the public, either directly or indirectly through data centers (both inside and outside the Kingdom) and manages them in whole or in part."

[11] See 1Password, "1Password Security Design"

1Password hosts a customer's encrypted data on its servers, but its zero-knowledge architecture means that it cannot access the customer's keys for encrypting the data; users create and store their own keys, using their choice of endpoints and underlying IT infrastructure.

Conclusion

1Password's zero-knowledge architecture empowers customers to manage credential sprawl while maintaining control of their encryption keys. While businesses should consult with their legal counsel before adopting any new tooling, this document finds that how 1Password's zero-knowledge architecture advances the security and resilience goals of Saudi Arabia's policy and regulatory framework for cybersecurity and digital sovereignty.

About the Author

1Password commissioned this study from Andrew J. Grotto, an independent expert in cybersecurity with extensive experience in the public, private, and academic sectors.

Grotto founded and co-directs the Program on Geopolitics, Technology, and Governance at Stanford University's Center for International Security and Cooperation (CISAC), and serves as the faculty lead for the Cyber Policy and Security specialization within Stanford's Ford Dorsey Master's in International Policy Program. He is a visiting fellow at the Hoover Institution and senior fellow for cybersecurity (non-resident) at the National Bureau of Asian Research.

Grotto is also President and CEO of Sagewood Global Strategies LLC, a technology policy and risk advisory firm. He sits on the Board of Directors for Slamfire Inc., the studio behind the AAA video game Back4Blood.

Before coming to Stanford in 2017, Grotto served in the executive and legislative branches of the U.S. government, most recently as the Senior Director for Cyber Policy on the National Security Council at the White House for two U.S. presidents.

The views presented here are the author's alone.