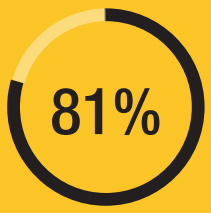
keeper

Keeper Enterprise

Uw grootste beveiligingsdreiging loopt elke dag bij u binnen.

Werknemers gebruiken zwakke werkwoorden, hergebruiken ze voor verschillende accounts en vergeten ze.



van de gegevenslekken zijn het gevolg van zwakke, standaard of gestolen wachtwoorden[1]

van de mensen gebruikt hetzelfde wachtwoord voor alles[2]

van de telefoontjes naar de helpdesk heeft betrekking op wachtwoorden[3]

Beveiliging

De meest geavanceerde beveiligingsgrens wordt eenvoudig overschreden als er zwakke wachtwoorden worden gebruikt. De wachtwoordgebruiken van werknemers kunnen alleen worden verbeterd met inzicht in het wachtwoordgebruik en naleving. Keeper lost dit op door uitgebreide rapportage, controle en meldingen te bieden.

Naleving

Voor elk cyberbeveiligingsframework, van NIST tot ISO en PCI tot HIPAA, is het traceren van toegang noodzakelijk, evenals toegang met minimale bevoegdheden en controlelogs. Keeper maakt op rollen gebaseerde controles en zichtbaarheid in gedeelde aanmeldingsgegevens mogelijk. U kunt de toegangslogs tot Keeper-kluizen controleren omwille van de naleving of forensische redenen.

Synchronisatie met Microsoft Active Directory

Keeper AD Bridge™ synchroniseert Microsoft Active Directory of Open LDAP. Hiermee wordt snelle gebruikerstoevoeging ingeschakeld en worden automatisch knooppunten (organisatorische eenheden), gebruikers, rollen en teams toegevoegd. Keeper schakelt op rollen gebaseerde toegangscontrole in, plus de mogelijkheid om rollen te volgen wanneer mensen van positie wisselen in de organisatie. Dit is inclusief de automatische vergrendeling van kluizen van werknemers die vertrekken.

Supportkosten

Verlaag de helpdeskkosten in verband met wachtwoordproblemen drastisch. Forrester heeft ontdekt dat grote bedrijven jaarlijks meer dan 1 miljoen dollar uittrekken voor wachtwoordgerelateerde support.

Productiviteit

Voorkom dat werknemers tijd verspillen en gefrustreerd raken, en verwijder de behoefte voor hen om wachtwoorden te hergebruiken en onthouden. Keeper genereert sterke, willekeurige wachtwoorden en vult ze automatisch in voor gebruikers. De Keeper-kluis, met een responsieve en intuïtieve UI, is beschikbaar voor werknemers vanaf elk apparaat en elke locatie. Alles wat Keeper doet is gericht op snelle toepassing door gebruikers en beveiliging. Keeper wordt gepubliceerd in 19 talen voor wereldwijd gebruik.

Automatisering van back-end-wachtwoordroulering

Keeper Commander SDK™ biedt IT-beheerders en -ontwikkelaars hulpmiddelen zoals opdrachtregels en Python-broncode voor wachtwoordbeheer, wachtwoordroulering en kluisfunctionaliteit. Elimineer hard-coded of tekstgebaseerde back-end-wachtwoorden. Connectoren zijn onder meer Unix, Windows en AD-aanmeldingen; Oracle, Microsoft SQL, MySQL,Postgres en Dynamo-databases; en AWS-wachtwoord en API-toegangscodes.

Duizenden organisaties vertrouwen op Keeper

Peapod · Chipotle Mexican Grill · Marks & Spencer · Toyota · UAB

> **Wachtwoordbeheeroplossingen voor ondernemingen kunnen helpen bij de beheersing van kosten en de realisatie van aantrekkelijke ROI** - Forrester[4]

Twee-factor-authenticatie

Keeper ondersteunt twee-factor-authenticatie (2FA), waaronder sms, Keeper DNA® (smartwatch), TOTP (bijvoorbeeld Google Authenticator en Authy), FIDO U2F (bijvoorbeeld Yubikey), Duo en RSA SecurID. 2FA kan worden afgedwongen door op rollen gebaseerde besturing.

Zero-knowledge architectuur

Alle versleuteling en ontcijfering vindt plaats op het apparaat van de gebruiker. PBKDF2 met 100.000 rondes wordt gebruikt om een code te verkrijgen van het hoofdwachtwoord van de gebruiker. Elke record is versleuteld met AES-256 met een andere en unieke code die willekeurig wordt gegenereerd door de client. RSA-versleuteling wordt gebruikt om veilig records te delen tussen gebruikers en teams. De infrastructuur van Keeper synchroniseert versleutelde tekst tussen apparaten. Key pinning wordt afgedwongen tussen client en server. Alle gegevens die onderweg zijn en in ruste worden altijd versleuteld - ze kunnen niet worden bekeken door Keeper Security-medewerkers of een externe partij.

Automatische toevoeging via e-mail

Grote organisaties zoals universiteiten kunnen Keeper-kluizen aanbieden aan duizenden gebruikers met e-mailadressen binnen hetzelfde domein. Met minimale administratie kan grootschalige inzet worden bereikt via een bestaand e-mailkanaal of bestaande portal.

Ondersteuning voor gelieerde ondernemingen, afdelingen, kantoren en filialen

Keeper is gemaakt om knooppunten en organisatorische eenheden te ondersteunen, om zo organisaties van elke grootte en binnen alle grote industrieën te bedienen. De Keeper-beheerder kan beleid voor wachtwoordbeheer structureren op rol, team en organisatorische eenheid. Op die manier kunnen verschillende divisies, branches, merken en kantoorlocaties van een organisatie allemaal beschermd worden met Keeper. Verschillende toegangsrechten, machtigingen en beleidsregels voor het afdwingen van veilig wachtwoordbeheer in de organisatie is mogelijk. Elke organisatie kan meerdere Keeper-beheerders inzetten met afgestemde machtigingen voor hun gebruikers, rollen en teams.

Keeper integreert met toonaangevende SSO-oplossingen

Keeper SSO Connect™ integreert met uw IdP en is de perfecte oplossing voor toepassingen die geen SAML-protocollen ondersteunen. Keeper biedt gebruikers daarnaast geprivilegieerde toegang, een veilige kluis om al hun niet-SSO-wachtwoorden in op te slaan, digitale certificaten, coderingssleutels en API-toegangssleutels.

Microsoft Azure · onelogin · ADFS · G Suite · okta · Centrify · amazon web services · JumpCloud · IBM Security · Ping Identity · f5

Verklaringen van derden en certificeringen over Keeper

GSA Schedule 70 Contract 47QTCA18D00C9 · TRUSTe CERTIFIED PRIVACY · AICPA SOC · PCI DSS COMPLIANT

[1] Verizon 2017 Incidentenrapport gegevenslekken [2] Keeper-enquête onder 1000 internetgebruikers in 2017 [3] Gartner Group [4] Forrester-rapport met best practices: selectie, implementatie en beheer van wachtwoordbeheerders voor ondernemingen

Ondersteuning

Amerika en APAX (consument)
+1 312 971 5702

Amerika en APAX (zakelijk)
+1 312 226 4782

EMEA (zakelijk)
+353 21 229 6019

ProteQtor
Next-Gen IT Security

ProteQtor IT Security is reseller van Keeper cybersecurity oplossingen.

Vragen of opmerkingen? Neem gerust contact met ons op!

BEL ONS
+31 (0)88 066 0770

VIND ONS
Industrieweg 20-7
3846 BD Harderwijk

MAIL ONS
info@proteqtor.nl