

CASESTUDY

Wereldwijd IT-bedrijf verbetert de beveiliging en naleving met Keeper



Achtergrond

De organisatie is een technologiebedrijf met klanten in verschillende sectoren, waaronder financiën, telecommunicatie, media, retail en gezondheidszorg.

Industrie

Technologische diensten

Werknemers

11.000+

Oplossingen

Enterprise Password Manager

- Platinum Support



De uitdaging

Als snelgroeiend bedrijf met een wereldwijd personeelsbestand, voelde de organisatie sterk de behoefte om de wachtwoordbeveiliging te verhogen. Werknemers gebruikten verschillende oplossingen voor wachtwoordbeheer, wat leidde tot fragmentatie, inconsistentie en een gebrek aan inzicht in het beheer van inloggegevens.

Bovendien wilden IT-beheerders best practices voor beveiliging delen met verschillende afdelingen. Toen de organisatie de ISO-normen en andere cybersecuritystandaarden verbeterde, zorgde het gebrek aan een uniforme oplossing voor wachtwoordbeheer voor hiaten in naleving en administratieve inefficiëntie.

De belangrijkste uitdagingen waren:

Beperkte zichtbaarheid en toegangscontrole: werknemers gebruikten verschillende tools, zoals [browsergebaseerde wachtwoordmanagers](#), waardoor beveiligingshandhaving en het handhaven van de datakwaliteit moeilijk werden.

Nalevingsvereisten en beveiligingsrisico's: om te voldoen aan de voortdurende verbeteringen van de ISO- en cybersecurity-certificeringsstandaarden was een gestructureerde oplossing op ondernemingsniveau nodig. De organisatie had meer zichtbaarheid nodig in de kwaliteit van inloggegevens en een naadloze manier om best practices voor gegevensbeveiliging af te dwingen..

We wilden ons wachtwoordbeheer verenigen onder een veilige oplossing die ons cybersecurity-team kon beoordelen en beheren.

- Jefe de Gestión de Entrega de Proyectos



De oplossing van Keeper

De organisatie evalueerde meerdere oplossingen voor wachtwoordbeheer voordat zij voor Keeper Security koos. Keeper viel op als een van de veiligste en meest uitgebreide opties en bood wachtwoordbescherming op ondernemingsniveau, veilig delen van inloggegevens en beste beveiliging in zijn categorie. De oplossing van Keeper biedt veel voordelen, waaronder:

Gecentraliseerd wachtwoordbeheer - Keeper voorzag de organisatie van een veilig platform voor het opslaan en beheren van de wachtwoorden van de organisatie. Dit zorgde ervoor dat alle inloggegevens werden beschermd met de [zero-trust en zero-knowledge](#) architectuur van Keeper.

Gebruikersacceptatie en training - Keeper wordt erkend als de toonaangevende wachtwoordmanager voor organisaties van elke omvang en is ontworpen om eenvoudig te gebruiken en snel te implementeren. Het uitgebreide [documentatieportaal](#) van Keeper biedt gedetailleerde instructies en beste gewoonten voor het systeem om beheerders te helpen om het meeste uit hun implementatie te halen. Voor eindgebruikers zorgen gedetailleerde [producthandleidingen](#) en [trainingsvideo's](#) voor een hoge acceptatie door gebruikers.

We hebben ons team zowel training voor eindgebruikers als training voor beheerders aangeboden. Het is een vrij intuïtieve interface en we hadden een echt soepele implementatie.

- Hoofd Project Delivery Management

Geavanceerde beveiligingsfuncties - de robuuste beveiligingsmaatregelen van Keeper, waaronder multifactorauthenticatie (MFA) en end-to-end versleuteling, zorgen ervoor dat gevoelige interne communicatie en gegevens worden beschermd. De mogelijkheid om inloggegevens veilig en naadloos te delen met team-leden zonder gevoelige gegevens bloot te stellen voegt een extra beschermingslaag toe.

Kosteneffectief - ongeacht de grootte of het type organisatie, Keeper heeft een kosteneffectief plan dat aansluit op de behoeften van de organisatie. Dankzij het transparante prijsmodel van Keeper en de hoogwaardige klantenondersteuning - beoordeeld als beste in Enterprise Customer Support op [G2](#) - halen organisaties het maximale uit hun investering.

Hoogwaardige beveiliging - onze zero-trust en zero-knowledge beveiligingsarchitectuur is ongeëvenaard in het beschermen van informatie en het beperken van het risico op een datalek. Keeper combineert elliptische curve-cryptografie (ECC) op [apparaatniveau met meerdere versleutelingslagen](#) (op kluis-, map- en recordniveau), multifactor- en biometrische authenticatie, en FIPS 140-3-gevalideerde AES 256-bits versleuteling in combinatie met PBKDF2. Keeper voldoet aan [SOC 2 en ISO 27001](#), met de langstlopende naleving in de branche, en is FedRAMP- en StateRAMP-geautoriseerd.



Impact op de organisatie

Door Keeper organisatiebreed te implementeren - bij een wereldwijd verspreid personeelsbestand van meer dan 11.000 medewerkers - kreeg de organisatie gecentraliseerde controle over wachtwoord- en toegangssleutelbeveiliging. Hierdoor kon het IT-team een sterk wachtwoordbeleid afdwingen, de hygiëne van inloggegevens controleren en veilig toegangsbeheer vergemakkelijken. De belangrijkste resultaten waren:

Sterkere beveiliging en conformiteit - Keeper verbeterde de beveiligingshouding van de organisatie en zorgde voor naleving van veel standaardcertificeringen, zoals ISO-certificeringsvereisten. IT-beheerders kunnen nu het gecentraliseerde dashboard van Keeper gebruiken om de beveiliging van inloggegevens in realtime te controleren.

Gestroomlijnde onboarding en offboarding - met Keeper kan de toegang tot inloggegevens naadloos worden toegewezen of ingetrokken tijdens het on- of offboardingproces. Dit, samen met de implementatie van Keeper in de hele organisatie, heeft de samenwerking en operationele efficiëntie gestroomlijnd.

Gebruikersadoptie en naadloze samenwerking - de intuïtieve interface en het gebruiksgemak van Keeper hebben geleid tot hoge adoptiepercentages, vooral onder niet-technisch personeel. Keeper biedt ook een gratis [gezinsabonnement voor alle zakelijke gebruikers](#), wat de adoptie versnelt. De gebruiksvriendelijke browserextensie vereenvoudigt wachtwoord- en passkeybeheer, verbetert de samenwerking tussen afdelingen en vermindert obstakels bij het verkrijgen van toegang tot gedeelde records.

Het team kon het erg waarderen dat Keeper een gratis gezinsabonnement bood. Het was een extra voordeel dat de gebruikersacceptatie nog sneller maakte.

- Hoofd Project Delivery Management

Beveiliging en zichtbaarheid - de organisatie integreerde Keeper naadloos met haar [SSO-provider](#), waardoor werknemers zich konden authenticeren voor Keeper met hun SSO-inloggegevens en veilige toegang konden krijgen tot de cloud- en lokale applicaties van de organisatie die SSO niet ondersteunen. [KeeperFill](#)® - een functie voor de browserextensie, de mobiele app en de desktoptoepassing van Keeper - stelt gebruikers in staat om inloggegevens direct automatisch in te vullen voor websites en apps.

Deze integratiemogelijkheden en het gebruiksgemak, samen met de toonaangevende beveiliging en zero-knowledge beveiligingsarchitectuur van Keeper, bood de organisatie een veilige oplossing voor wachtwoordbeheer om te beschermen tegen cyberbedreigingen.



Keeper Password Manager

De meeste bedrijven hebben een beperkt inzicht in de wachtwoordgewoonten van hun werknemers, waardoor het cyberrisico sterk kan worden verhoogd. De wachtwoordetiquette kan niet worden verbeterd zonder kritieke informatie te hebben over wachtwoordgebruik en naleving. Keeper lost dit op door ultieme beveiliging, zichtbaarheid en controle te bieden.

Gegevens worden beschermd met de zero-knowledge beveiligingsarchitectuur en de hoogwaardige versleuteling van Keeper. Zero-knowledge betekent dat alleen de gebruiker kennis heeft van en toegang heeft tot hun hoofdwachtwoord en de versleutelingssleutel die wordt gebruikt voor de versleuteling en ontsleuteling van hun gegevens.

Keeper is intuïtief en eenvoudig te implementeren, ongeacht de grootte van het bedrijf. Keeper integreert met Active Directory- en LDAP-servers, waardoor toegangsverlening en onboarding worden gestroomlijnd. [Keeper SSO Connect®](#) wordt geïntegreerd in bestaande SSO-oplossingen en is FedRAMP- en StateRAMP-geautoriseerd.

Keeper is ontworpen om mee te schalen met organisaties van elke omvang. Functies zoals rolgebaseerde machtigingen, teamdelen, afdelingsauditing en gedelegeerd beheer bieden ondersteuning aan groeiende organisaties. [Keeper Commander](#) biedt robuuste API's om te integreren in huidige en toekomstige systemen.

Zakelijke use cases: Keeper Password Manager

- Voorkom wachtwoordgerelateerde gegevensinbreuken en cyberaanvallen
- Ondersteuning van passkeys voor moeiteloze authenticatie
- Betere naleving
- Verhoog de productiviteit van werknemers
- Dwing wachtwoordbeleid en -procedures af
- Verlaag de helpdeskkosten
- Minimaliseer training met snelle time-to-security
- Verbeter het beveiligingsbewustzijn en het gedrag van werknemers

Over Keeper

Keeper Security transformeert cybersecurity voor miljoenen individuen en duizenden organisaties wereldwijd. Het intuïtieve cybersecurity-platform van Keeper is gebouwd met end-to-end versleuteling en wordt vertrouwd door Fortune 100-bedrijven om elke gebruiker, op elk apparaat en op elke locatie te beschermen. Onze gepatenteerde zero-trust en zero-knowledge oplossing voor geprivilegieerd toegangsbeheer verenigt wachtwoord-, geheimen- en verbindingsbeheer van de onderneming met zero-trust netwerktoegang en externe browserisolatie. Door deze kritieke identiteits- en toegangsbeheercomponenten te combineren in één enkele cloudgebaseerde oplossing, biedt Keeper ongeëvenaarde zichtbaarheid, beveiliging en controle, samen met de garantie dat er aan alle nalevings- en auditvereisten wordt voldaan. Ontdek via [KeeperSecurity.com](#) hoe Keeper uw organisatie kan beschermen tegen de huidige cyberbedreigingen.

Keeper wordt wereldwijd vertrouwd en gewaardeerd door duizenden bedrijven en miljoenen mensen.



G2
Marktleider in het
enterprise-segment



PCMag
Selección del editor



App Store
Hoogst gewaardeerde
productiviteit



Google Play
Meer dan 10 miljoen
installaties