

CASE STUDY

Lucidica versterkt naleving en vertrouwen van klanten met KeeperMSP®



Achtergrond

Lucidica is een gevestigde Managed Service Provider (MSP) die end-to-end IT-ondersteuning, cybersecurity en adviesdiensten biedt aan kleine en middelgrote bedrijven in het Verenigd Koninkrijk.

Als vertrouwde IT-partner van tientallen organisaties hecht Lucidica veel waarde aan naleving, betrouwbaarheid en het vermogen om de beste beveiligingspraktijken voor haar klanten te implementeren. Om te voldoen aan de Cyber Essentials en ISO-nalevingsnormen, heeft het bedrijf een wachtwoordbeheeroplossing op bedrijfsniveau nodig die een veilige samenwerking binnen het gedistribueerde team mogelijk maakt.

Branche

Managed Service Provider (MSP)

Medewerkers

<50

Oplossingen

KeeperMSP® and BreachWatch



De uitdaging

Voordat Keeper werd ingevoerd, vertrouwde Lucidica op een verouderde wachtwoordbeheerder die vaak operationele vertragingen veroorzaakte en onnodige beveiligingsrisico's introduceerde. Hierdoor had de organisatie moeite om aan een aantal fundamentele vereisten te voldoen, wat de behoefte aan een veilige, gebruiksvriendelijke oplossing voor wachtwoordbeheer onderstreepte. De organisatie wendde zich tot Keeper om problemen van de vorige oplossing op te lossen, zoals:

Storingen bij kluisynchronisatie - Wachtwoorden verschenen vaak anders op verschillende apparaten, wat leidde tot verwarring en tijdverspilling terwijl technici probeerden de juiste inloggegevens te bepalen.

Inconsistente en onbetrouwbare wachtwoorddeling - Gedeelde aanmeldingsgegevens werden vaak niet gesynchroniseerd of kwamen helemaal niet aan. Als tijdelijke oplossing werd gevoelige informatie, waaronder creditcardnummers, uitgewisseld via e-mails, documenten en met wachtwoorden beveiligde spreadsheets. Deze onveilige methoden voor het delen van gegevens verhoogden het risico op het blootleggen van kritieke gegevens aanzienlijk.

Impact op klantadvies - Als MSP adviseert Lucidica regelmatig klanten over cyberbeveiliging. De tekortkomingen van het vorige systeem maakten het moeilijk om de best practices voor wachtwoordbeheer met vertrouwen te promoten.

“We moesten onze klanten het goede voorbeeld geven. Het vorige platform was niet alleen onbetrouwbaar — de problemen ontmoedigden klanten om wachtwoordmanagers überhaupt te gebruiken.”

Maria Nagle | Manager dienstverlening en projecten

Lucidica zag al snel de noodzaak in van een veilige en intuïtieve cloudoplossing die aansluit bij moderne operationele en nalevingsnormen in de Europese regio.



De oplossing van Keeper

Na verschillende platforms voor wachtwoordbeheer te hebben geëvalueerd, koos Lucidica voor **KeeperMSP** met de **BreachWatch-add-on**, waarmee ze toegang kregen tot wachtwoordbeheer op bedrijfsniveau en dark web-monitoring. De oplossing bood de naadloze, multi-tenant, cloudgebaseerde ervaring die het team miste en loste onmiddellijk de snelheids- en betrouwbaarheidsproblemen op die de vorige tool met zich meebracht.

Een groot voordeel was de Microsoft SSO-integratie van Keeper, die de authenticatiepraktijken versterkte en de onboarding van gebruikers vereenvoudigde. Lucidica merkte ook de hoge kwaliteit van de klantenservice van Keeper op. Van het eerste telefoongesprek tot de demonstratie en de uiteindelijke uitrol verliep het implementatieproces snel, soepel en veel efficiënter dan bij eerdere leveranciers.

“Alles ging snel — het eerste contact, de demonstratie en de installatie. Andere leveranciers konden er gewoon niet aan tippen.”

Nubia Coleman | algemeen directeur

KeeperMSP ondersteunde ook de toewijding van Lucidica op naleving van de Cyber Essentials en ISO-normen, en versterkte daarmee haar vermogen om als MSP sterke beveiligingsnormen aan klanten uit te dragen.

Kosteneffectief - Ongeacht de grootte of het type organisatie, heeft Keeper een kosteneffectief abonnement dat past bij en meegroeit met de behoeften van de organisatie. Het transparante prijsmodel van Keeper, gecombineerd met klantenservice van wereldklasse — beoordeeld als nummer 1 in Enterprise Customer Support op **G2** — zorgt ervoor dat organisaties hun investering maximaal benutten.

Beveiliging van wereldklasse - De zero-trust en zero-knowledge beveiligingsarchitectuur van Keeper is ongeëvenaard in het beschermen van informatie en het beperken van het risico op een gegevenslek. Keeper combineert Elliptic-Curve Cryptography (ECC) op apparaatniveau met **meerdere lagen van versleuteling** (op kluis-, map- en recordniveau), multi-factor- en biometrische authenticatie, evenals FIPS 140-3 gevalideerde AES 256-bits versleuteling en PBKDF2. Keeper is **SOC 2 en ISO 27001-conform** — met de langste aaneengesloten naleving in de sector — en tevens FedRAMP- en GovRAMP-geautoriseerd.

“Keeper is gemakkelijk te gebruiken en zeer gebruiksvriendelijk. De synchronisatie is snel en betrouwbaar.”

Maria Nagle | manager dienstverlening en projecten



Impact op de organisatie

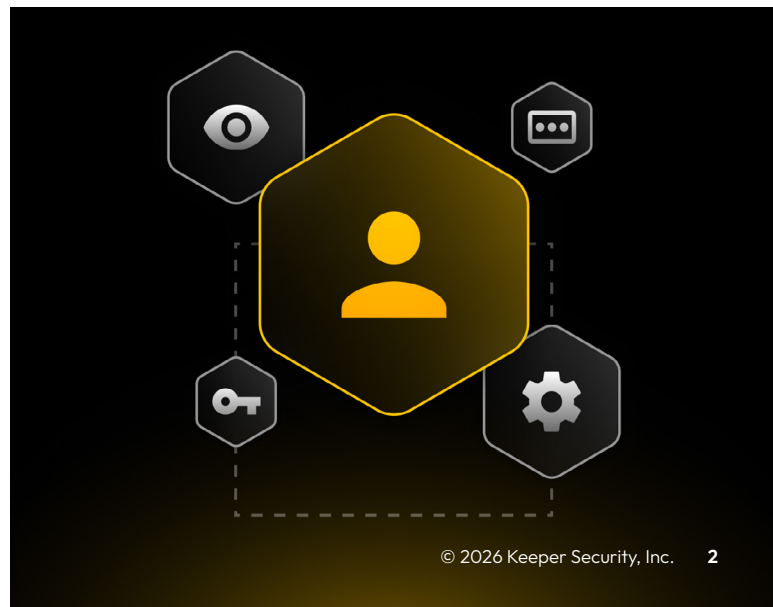
De implementatie van Keeper binnen het team verliep eenvoudig. Beheerders pasten zich snel aan het beheren van rollen, machtigingen en gedeelde mappen aan, en vinden het platform intuïtief en gebruiksvriendelijk. De trainingsvideo's en uitgebreide documentatie van Keeper hielpen Lucidica ook nieuwe medewerkers soepel te integreren en best practices met haar klanten te delen.

Ook voor de eindgebruikers was de ervaring positief. De browserextensie en autofill-mogelijkheden maakten alledaagse taken eenvoudiger, en het meegeleverde gezinsabonnement hielp zelfs om de cyberbeveiligingsgewoonten thuis te verbeteren.

Dark-webmonitoring - Toegevoegde functies zoals BreachWatch werden al snel essentieel voor de workflow van de organisatie en bieden realtime inzicht in gecompromitteerde aanmeldingsgegevens die op het dark web zijn gevonden. De Beveiligingsaudit hielp ook bij het opsporen van zwakke of hergebruikte wachtwoorden en bij het handhaven van een sterkere algemene hygiëne in het hele bedrijf.

Gestroomlijnde workflows - Omdat Keeper cloudgebaseerd is, heeft het team niet meer te maken met bevroren schermen, installatieproblemen of synchronisatiefouten, wat vaak voorkwam bij de vorige desktoptool. De realtime synchronisatie van Keeper maakte een einde aan inconsistente wachtwoorden en gebrek aan overzicht over verschillende apparaten, en maakte voortdurende probleemoplossing overbodig. Dit kwam de operationele efficiëntie ten goede.

Sinds de implementatie van Keeper heeft Lucidica een duidelijke verbetering in zowel haar beveiliging als haar productiviteit gerealiseerd. Het team vertrouwt niet langer op onveilige bestanden of berichtentools om wachtwoorden op te slaan of te delen, en synchronisatieproblemen zijn volledig geëlimineerd. De beveiliging en naleving van regelgeving zijn verbeterd, de gebruikerstevredenheid is hoog en Lucidica kan wachtwoordbeheer nu vol vertrouwen aan haar klanten aanbevelen — iets wat voorheen niet mogelijk was.





Keeper Password Manager

De meeste bedrijven hebben beperkt inzicht in de wachtwoordpraktijken van hun werknemers, waardoor het cyberrisico aanzienlijk wordt verhoogd. De wachtwoordhygiëne kan niet worden verbeterd zonder essentiële informatie over het gebruik van wachtwoorden en naleving. Keeper lost dit op door ultieme beveiliging, zichtbaarheid en controle te bieden.

Gegevens worden beschermd met de zero-knowledge beveiligingsarchitectuur van Keeper en versleuteling van wereldklasse. Zero-knowledge houdt in dat alleen de gebruiker kennis heeft van en toegang heeft tot diens hoofdwachtwoord en de encryptiesleutel die wordt gebruikt om diens informatie te versleutelen en te ontcijferen.

Keeper integreert met Active Directory- en LDAP-servers, wat het inrichten en onboarden stroomlijnt. **Keeper SSO Connect®** integreert in bestaande SSO-oplossingen en is FedRAMP- en GovRAMP-geautoriseerd. Keeper is ontworpen om mee te schalen met organisaties van elke omvang. Functies zoals rolgebaseerde machtigingen, teamdeling, afdelingsaudits en gedelegeerd beheer ondersteunen organisaties naarmate ze groeien. **Keeper Commander** biedt robuuste API's voor integratie met huidige en toekomstige systemen.

Waarom u **KeeperMSP** nodig heeft voor uw bedrijf:

- Gebruiksvriendelijk multi-tenantbeheer voor MSP's
- Wachtwoordgerelateerde gegevenslekken en cyberaanvallen voorkomen
- Passkeys ondersteunen voor moeiteloze authenticatie
- Klanttevredenheid vergroten
- Nieuwe inkomstenstromen genereren
- Wachtwoordbeleid en -procedures afdwingen
- Naleving en rapportage verbeteren
- Training minimaliseren met snelle implementatie van beveiliging
- Veiligheidsbewustzijn en -gedrag van werknemers verbeteren

OVER KEEPER

Keeper Security is een van de snelst groeiende cybersecurity-softwarebedrijven en beschermt meer dan 100.000 organisaties en miljoenen mensen in meer dan 150 landen. Keeper is een pionier op het gebied van zero-knowledge en zero-trust beveiliging, gebouwd voor elke IT-omgeving. Het kernaanbod, KeeperPAM®, is een AI-gebaseerd, cloud-native platform dat alle gebruikers, apparaten en infrastructuur beschermt tegen cyberaanvallen. Keeper is erkend voor zijn innovatie in het Gartner Magic Quadrant voor Privileged Access Management (PAM) en beveiligt wachtwoorden en sleutels, infrastructuurgeheimen, externe verbindingen en eindpunten met rolgebaseerd handhavingsbeleid, minimale privileges en just-in-time toegang. Ontdek waarom toonaangevende organisaties vertrouwen op Keeper om zich te beschermen tegen hedendaagse cyberdreigingen via [KeeperSecurity.com](https://keepersecurity.com).

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



G2
Enterprise Leader



PCMag
Editor's Choice



App Store
Eersteklas
productiviteit



Google Play
Meer dan 10 miljoen
installaties