



Қызметкерлердің
құпиясөздерін қауіпсіз
басқару

Бизнеске арналған Kaspersky Password Manager

kaspersky

60%

Ағып кеткен
құпиясөздердің бір
сағатта бұзуға болатын
үлесі¹

>20%

15 таңбалы
құпиясөздердің бір
минутта бұзуға болатын
үлесі¹



Бизнеске арналған Kaspersky Password Manager

Қызметкерлердің құпиясөздерін қауіпсіз басқару

Қазіргі компаниялар ондаған корпоративтік сервистер, қолданбалар мен жүйелерді пайдаланады. Оларға қол жеткізуді басқару, әсіресе үлестірілген инфрақұрылым, қашықтан жұмыс істеу және кибершабуылдар санының өсуі жағдайында күрделі міндетке айналууда. Өйткені бүгінгі таңда тіркелгі деректерінің бұзылуы — шабуылдаушылар үшін ең жиі кездесетін кіру нүктесі.

Бизнеске арналған Kaspersky Password Manager — бұл құпиясөздерді, құжаттарды, екінші фактор кодтарын, кіру кілттерін және қызметкерлердің басқа да құпия деректерін қауіпсіз сақтауға және пайдалануға арналған шешім.

Шешім тіркелгі деректерінің ағып кету тәуекелдерін азайтуға және пайдаланушылардың корпоративтік сервистермен ыңғайлы әрі қауіпсіз жұмыс істеуін қамтамасыз етуге көмектеседі.

Бизнеске арналған артықшылықтар



Құпия деректерді қорғау деңгейін арттыру

Тіркелгі деректерінің бұзылуы салдарынан ағып кету тәуекелін азайту



Қауіпсіздік инциденттерін тергеуді жеңілдету

Пайдаланушылардың барлық әрекеттерінің тарихын сақтау: құпиясөздерді экспорттау, оларды жаңарту және т.б.



Корпоративтік қауіпсіздік талаптарына сәйкестік

Құпиясөздерді басқару жөніндегі корпоративтік саясаттарға сәйкес енгізу және бақылау



Қызметкерлердің корпоративтік сервистермен қауіпсіз жұмыс істеуі

Пайдалану ыңғайлылығы және «адами фактордың» әсерін барынша азайту



Қызметкерлердің корпоративтік құпиясөздерін орталықтандырылған түрде басқару

Кіру деректерінің қалай пайдаланылатынының ашықтығы, пайдаланушылардың құқықтары мен қоймаларын басқару

Қызметкерлердің құпиясөздерінің өмірлік циклін басқару



Негізгі артықшылықтар



Zero-knowledge³ қағидаты бойынша End-to-end² шифрлау

Деректер шифрланған қоймада сақталады, оған тек негізгі құпиясөзі бар пайдаланушы ғана қол жеткізе алады



On-premises⁴ орналастыру

Шешім ұйымның инфрақұрылымында орналастырылады, осылайша деректерді толық бақылауға мүмкіндік береді



Толық функционалды клиенттік қолданба

Деректерді жергілікті өңдеу және шифрлау, браузерге қарамастан қолданбаның тұрақты жұмыс істеуі, тіпті сервермен байланыс үзілген жағдайда да қоймаға қол жеткізу мүмкіндігі сақталады

2 End-to-end шифрлау: ақпарат серверге жіберілмес бұрын тікелей пайдаланушы құрылғысында шифрланатын және оның шифрын тек уәкілетті алушы ғана аша алатын қорғау әдісі

3 Zero-knowledge: провайдердің пайдаланушы деректеріне қол жеткізуінсіз деректерді сақтау моделі

4 On-premises орналастыру: БҚ-ны компанияның жеке инфрақұрылымында орналастыру



Бизнеске арналған Kaspersky Password Manager

Қосымша
ақпарат

www.kaspersky.kz/kk

© 2026 АО "Лаборатория Касперского".
Тіркелген тауар белгілері мен қызмет көрсету
белгілері олардың тиісті құқық иеленушілерінің меншігі
болып табылады.

#kaspersky
#болашақтыбелсендір