DASHLANE

BESCHERMING VAN TOEGANGSGEGEVENS

Ontdek risico's. Bestrijd bedreigingen.

De diefstal van toegangsgegevens is in 2024 met 703% gestegen[1]. Om beschermd te blijven, moeten organisaties begrijpen waar hun risico's voor toegangsgegevens zitten en snel handelen, voordat ze actieve bedreigingen worden.

Credential Protection, beschikbaar op het Dashlane Omnix™-platform, koppelt altijd-actieve toegangsgegevensintelligentie aan gerichte acties om te beschermen tegen de grootste inbreukbedreiging: risicovolle toegangsgegevens van medewerkers.

$4,44 miljoen

is de gemiddelde kost van een gegevenslek[2]

Met bescherming van toegangsgegevens kunt u:

Risico's identificeren

Risicodetectie voor toegangsgegevens biedt beheerders inzichten in elk risicovol toegangsgegeven, zelfs als medewerkers Dashlane niet gebruiken. In één maand wist een organisatie het aantal gecompromitteerde toegangsgegevens met 75% te verminderen.

Automatiseer risicorespons

Nudges verminderen de IT-werkbelasting met geautomatiseerde browser- en Slack-meldingen die medewerkers aansporen om risicovolle wachtwoorden te updaten. Ze bieden "het juiste niveau van begeleiding zonder wrijving te veroorzaken", deelt een beheerder.

Phishing-aanvallen te slim af zijn

AI-waarschuwingen voor phishing detecteren phishing-risico's in minder dan een halve seconde met behulp van een eigen AI-model en sturen medewerkers een contextuele waarschuwing op het moment dat ze een verdachte site bezoeken, zelfs als ze niet zijn ingelogd op Dashlane.

Stop met het spelen van detective. Onderneem actie.

Neem contact op met Sales voor meer informatie.

1. SlashNext's 2024 Phishing Intelligence-rapport
2. IBM's 2025 Kosten van een gegevenslekrapport