



LastPass voor de gezondheidszorg

De gezondheidszorg is een breed werkveld, met ziekenhuizen, artsenpraktijken, thuiszorgbureaus, farmaceuten, producenten van medische apparatuur, zorgverzekeraars, GGD's, onderzoeksinstellingen en meer. De sector omvat een enorm breed netwerk van professionals, faciliteiten en technologieën.

Ook zorgsystemen hebben goede zorg nodig

Zorgverleners hebben een belangrijke verantwoordelijkheid om de gevoelige gegevens van hun patiënten, klanten en samenwerkingspartners veilig te houden. Hun systemen bieden onder andere toegang tot medische gegevens, patiëntendossiers, onderzoeksresultaten en financiële informatie. Cybercriminelen hebben het steeds vaker voorzien op de gezondheidszorg, waar een slechte omgang met wachtwoorden en ontoereikende toegangscontroles de deur vaak open zetten voor hackers. Als medewerkers of inhuurkrachten onnodig toegang krijgen of toegang niet op tijd wordt ingetrokken, vergroot dit het risico op ongeoorloofde toegang en beveiligingsproblemen.

Zorgorganisaties die overstappen op de cloud, worstelen met goed wachtwoordbeheer voor de groeiende hoeveelheid platformen en tools. Systemen zijn kwetsbaar door ondoordachte configuraties, gedateerde werkstations en onbeveiligde gedeelde apparaten. En cybercriminelen maken hier dankbaar gebruik van, bijvoorbeeld door ziekenhuizen lam te leggen met ransomware. Zonder gecentraliseerd wachtwoordbeheer is het onmogelijk om dit soort aanvallen effectief af te weren.

Ook compliance is een punt van zorg, en de Autoriteit Persoonsgegevens is streng voor zorgorganisaties die steken laten vallen. Goed wachtwoordbeheer kan ransomware, boetes en reputatieschade vermijden. Zorgorganisaties die hun aanmeldingsgegevens en toegangsrechten niet goed op orde hebben, riskeren problemen met hun gegevensbescherming, compliance en ook met hun cyberverzekering.

Het Amerikaanse Department of Health and Human Services (DHHS) zag een toename in grote gegevenslekken van 93% tussen 2018 en 2022. Grote ransomware-aanvallen namen in deze periode toe met 278%.

Eerste hulp voor wachtwoorden: LastPass



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en heeft unieke mogelijkheden om zorgprofessionals te helpen met hun cyberbeveiliging. De software is speciaal gemaakt voor de complexe behoeften van werkplekken met veel accounts en systemen. Met LastPass kunnen zorgorganisaties sterke wachtwoorden maken, opslaan en beheren, en veilig toegang delen waar nodig. De handige interface versterkt de beveiliging en verhoogt tegelijkertijd het gebruiksgemak. Zwakke of onbeheerde wachtwoorden zijn verleden tijd, en zorgverleners kunnen zich weer concentreren op hun patiënten of hun onderzoek.



Beveiligingssoftware kan alleen goed werken als het in de praktijk ook handig is voor IT-beheerders, behandelaars, en bijvoorbeeld inhuurkrachten, onderzoekers en samenwerkingspartners. LastPass levert dit gebruiksgemak. Het werkt in de cloud en maakt de omgang met wachtwoorden niet alleen veilig, maar ook eenvoudig. Gevoelige gegevens worden goed beveiligd, terwijl geautoriseerde gebruikers eenvoudig kunnen inloggen en waar nodig toegang ook veilig kunnen delen met anderen. IT-beheerders in de zorg kunnen LastPass gebruiken om een gestructureerd beveiligingsbeleid op te zetten dat ongeoorloofde toegang blokkeert, risico's door kwaadwillende insiders vermindert, en menselijke fouten elimineert.



De krachtige rapportagefunctie maakt het bovendien mogelijk om te volgen wie er wanneer toegang heeft gehad tot welke gegevens. Dit helpt om afwijkend gedrag op te sporen, en het ondersteunt de compliance. Met LastPass kunnen organisaties niet alleen de groeiende digitale bedreigingen voor de zorg het hoofd bieden, maar ook hun dagelijkse werkprocessen stroomlijnen en toezichthouders tevreden stellen.

Voordelen van LastPass voor de gezondheidszorg

De makkelijkste, meest betaalbare en meest betrouwbare manier voor zorgprofessionals om hun cyberrisico en operationele risico terug te dringen, is door hun wachtwoordbeheer organisatiebreed te organiseren met LastPass.

Beveiliging	Voorkom ongeoorloofde toegang	Houd hackers en ongeoorloofde gebruikers buiten uw toepassingen, online accounts, gevoelige gegevens en systemen.
	Blokkeer overnames van uw accounts en gegevenslekken	Zorg dat online accounts en toepassingen betrouwbaar toegankelijk zijn voor geautoriseerde gebruikers en dat aanmeldingsgegevens beschermd blijven.
	Krijg schaduw-IT onder controle	Krijg zicht op toepassingen die medewerkers gebruiken zonder toestemming en beheer van de IT-afdeling. Voorkom onnodige abonnementen en volg wie er aanmeldingsgegevens deelt voor welke accounts. Beheer de toegangsrechten en herken kwetsbaarheden in het systeem.
	Breid veilig toegangsbeheer uit	Integreer naadloos met identiteitsproviders als Microsoft Entra en verbeter het gebruikersbeheer van inhuur tot aan vertrek.
Naleving	Voldoe aan voorwaarden van cyberverzekeraars	Toon eenvoudig aan dat u voldoet aan de vereisten die cyberverzekeraar stellen aan wachtwoord- en toegangsbeheer.
	Ondersteun compliance	Voldoe aan de vereisten van wet- en regelgeving, onder andere voor de AVG, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA en SOX, en voor kaders voor cyberbeveiliging zoals NIST, CISA, Zero Trust, en NERC-CIP.
	Garandeer de beveiliging die partners vereisen	Voldoe aan de strenge beveiligingsvereisten van partners, met krachtige systemen voor toegangscontrole, regels voor het delen van wachtwoorden, sterke verificatiemechanismen en nuttige rapportages.
Optimalisatie	Bied iedereen een intuïtieve gebruikservaring	Profiteer van uitgebreide instelbare beleidsregels, flexibele machtigingen, gedetailleerde rapportages, en verschillende opties voor de verificatie.
	Standaardiseer de wachtwoordbeveiliging	Vereenvoudig het wachtwoordbeheer voor alle medewerkers binnen de organisatie.
	Verlaag de werkdruk voor de helpdesk	Verlos de helpdesk van problemen door aanmeldingsgegevens, zoals vergeten wachtwoorden en geblokkeerde accounts.
Samenwerking	Stroomlijn teamwerk met gedeelde toegang	Maak het makkelijk om wachtwoorden en andere informatie zowel intern als extern veilig te delen, voor meer productiviteit en efficiency voor partners, freelancers en thuiswerkers.
	Optimaliseer aanname & gebruik	Bevorder de aanname en het gebruik door medewerkers met een intuïtieve, gebruiksvriendelijke interface, die alle taken rondom wachtwoordbeheer makkelijker maakt.
	Bouw een veiligheidscultuur	Zorg ervoor dat alle medewerkers actief bijdragen aan een hoog veiligheidsbewustzijn en de organisatie beschermen tegen veel voorkomende bedreigingen rondom gestolen of gelekte aanmeldingsgegevens.