Kensington®

Vergeet je wachtwoord

De veiligste log-in is binnen handbereik

Uw werknemers vormen de grootste bedreiging voor de beveiliging van uw data.

Gegevensinbreuken nemen toe. Naar schatting zijn er in 2019[1] 8,5 miljard gegevensinbreuken geweest, een stijging van 70% ten opzichte van 2018.[2]

Hacking (het gebruik van exploits om toegang te krijgen tot bevoorrechte informatie) en phishing (het zich voordoen als een betrouwbare bron zodat vertrouwelijke gegevens worden ingeleverd) zijn de meest voorkomende cyberaanvallen die worden gebruikt om gegevensinbreuken te veroorzaken. **80% van de hackinggerelateerde overtredingen wordt veroorzaakt door gecompromitteerde, zwakke en hergebruikte wachtwoorden.[3]**

'Veilige' wachtwoorden - met hoofdletters, kleine letters, cijfers en symbolen - worden heel snel vergeten. Gezien het feit dat de gemiddelde zakelijke gebruiker 191 wachtwoorden4 heeft, zijn ze een echte uitdaging om te beheren.

In plaats van alleen te vertrouwen op gebruikersnamen en wachtwoorden, creëert Multi-Factor Authenticatie (MFA) een extra beveiligingslaag. **De biometrische authenticatie is het meest veilige niveau van MFA en vereist een extra factor om toegang te verlenen.**

MFA kan naadloos worden geïmplementeerd in gebruikersworkflows met Windows Hello die biometrische log-in en wachtwoordloze toegang tot online diensten ondersteunt. De FIDO Alliance heeft normen opgesteld om de compatibiliteit van apparaten te maximaliseren.

Kensington VeriMark™ USB Fingerprint Key

- ☑ Biometrische log-in
- ☑ Ondersteunt MFA
- ☑ Windows Hello
- ☑ FIDO U2F gecertificeerd

Kensington®

Het is tijd om je wachtwoord te vergeten

Single-factor authenticatie - met andere woorden, een wachtwoord dat geen extra verificatie vereist - wordt door hackers gezien als het pad van de minste weerstand. Wanneer een phishingcampagne of replay-aanval met succes een wachtwoord oogst, kan er nog meer informatie worden gekaapt wanneer de toegang tot het apparaat wordt gecompromitteerd.

Wachtwoorden, zelfs sterke, zijn niet langer voldoende om gevoelige accounts en activa te beschermen tegen hacking en phishing-aanvallen.

Er bestaat een nauw verband tussen alleen de beveiliging van wachtwoorden en gegevensinbreuken, aangezien beide een vicieuze cirkel van dure informatiediefstal bestendigen.

Uw wachtwoorden zijn niet veilig genoeg

Zonder extra veiligheidsmaatregelen zijn wachtwoorden kwetsbaar voor routinematige diefstal en onderschepping. **Twee-factor-authenticatie** (of multifactor-authenticatie) moet deel uitmaken van elke moderne set authenticatieprotocollen.

Door naast een wachtwoord een extra stukje informatie (of factor) te vragen, of twee stukjes unieke informatie zonder enig wachtwoord, vermijdt 2FA/MFA de bekende complexiteiten en tekortkomingen van wachtwoordgeoriënteerde log-ins.

Unieke biometrische gegevens, zoals vingerafdrukken, zijn superieur aan traditionele sms-teksten en veiligheidsvragen, die kunnen worden onderschept zonder dat de gebruiker het weet. De authenticatietechnologie is geëvolueerd met de introductie van biometrische oplossingen zoals Microsoft's Windows Hello log-in[5] , compatibel met **Kensington's VeriMark™ Fingerprint Key.**

Waarom 2FA en MFA?

De fundamentele fout van single-factor wachtwoordbeveiliging is dat als een ongeautoriseerde partij de juiste login heeft, zij toegang heeft tot het met een wachtwoord beveiligde account. **Het maakt niet uit of ze het wachtwoord hebben verkregen door diefstal, een systematische woordenboekaanval of een gelukkige gok: het resulterende risico is hetzelfde.**

De tweede en multifactor authenticatie verandert het authenticatiemodel op twee verschillende manieren ten goede:

- **Vereist verificatie van een ander gegeven na succesvolle invoer van een wachtwoord.**
- **Het inloggen wordt uitsluitend toegestaan door middel van een veiliger wachtwoordloos mechanisme.**

In beide gevallen zal de authenticatieoplossing proberen de identiteit van een **gebruiker te verifiëren door te vragen om iets wat hij kent, heeft of waarmee hij kan worden geïdentificeerd.** De mogelijkheden variëren van een eenmalig wachtwoord dat via sms wordt verstuurd of in een authenticatie-applicatie wordt gegenereerd, tot iets wat aanzienlijk sterker is, zoals een hardware of een vingerafdruksleutel. De laatste twee bieden meer veiligheid omdat ze niet kwetsbaar zijn voor onderschepping of phishing.

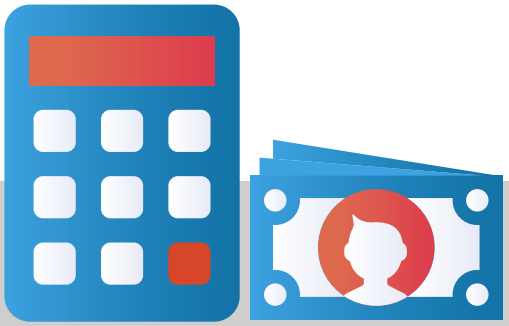
De voordelen van Biometrie voor 2FA, MFA en Wachtwoordloze Log-Ins

Biometrie biedt een unieke combinatie van gemak en veiligheid om de volgende redenen:

- **Ze zijn eenvoudig te scannen, te verifiëren en te associëren met een specifieke identiteit.**
- **Ze zijn gebaseerd op gegevens die moeilijk te dupliceren of te stelen zijn.**
- **Ze worden opgeslagen of overgebracht via gespecialiseerde hardware, om toegang op afstand of diefstal te voorkomen.**

Biometrische authenticatie kan meer opleveren dan alleen een betere inlogervaring voor eindgebruikers.

Biometrie maakt het mogelijk om zonder wachtwoord in te loggen, waardoor de belasting van de IT-helpdesk door het resetten van wachtwoorden wordt verminderd. Elke wachtwoordreset kost naar schatting meer dan €60[6] - en meer dan 40% van de gebruikers heeft 50+ resets per jaar nodig.[7]



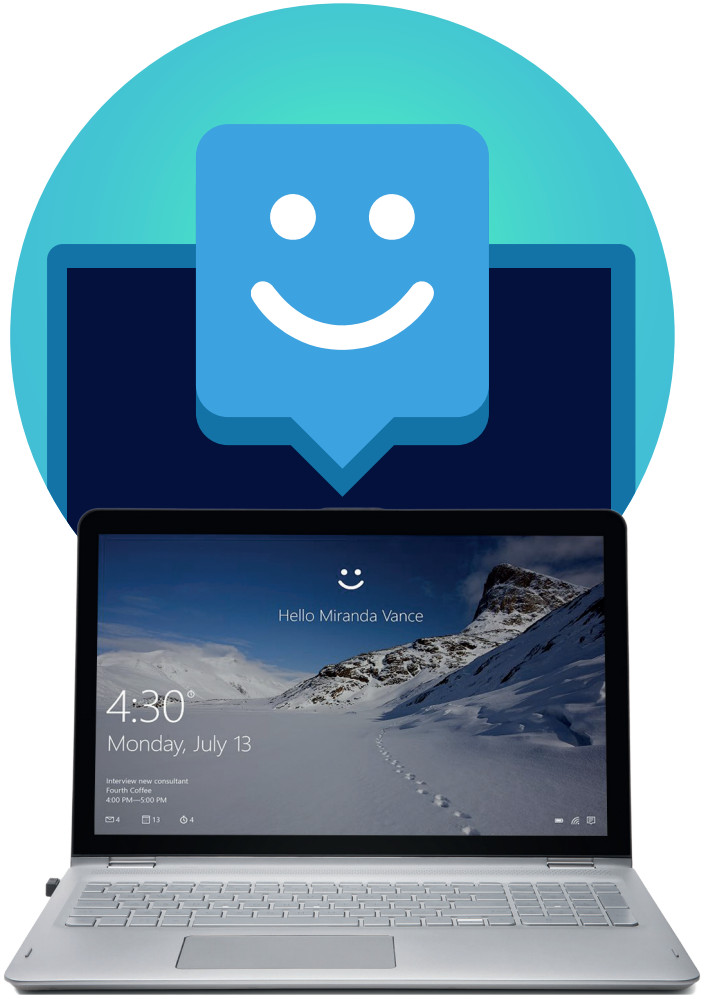
In een organisatie met 1000 gebruikers is dat samen goed voor €1.2 miljoen per jaar aan verloren tijd en productiviteit.

Windows Hello Ondersteunt Direct Biometrisch inloggen

Windows Hello, een standaardfunctie van Windows 10, ondersteunt direct biometrisch inloggen. Deze biometrische opties omvatten gezichtsherkenning, irisscanning en het lezen van vingerafdrukken, **dit laatste via FIDO U2F-gecertificeerde hardware zoals de Kensington VeriMark™ Fingerprint Key.**

Windows Hello elimineert het ongemak van het maken en onthouden van complexe wachtwoorden. Nog belangrijker is dat het de gebruikelijke mazen in de beveiliging op basis van een wachtwoord vermijdt, zoals het blootleggen van inloggegevens via phishing.

De inlogervaring voor Windows Hello is zeer eenvoudig. Succesvolle biometrische authenticatie ontgrendelt de toegang tot een ondersteund Windows apparaat.



Wat is FIDO?

De **Fast IDentity Online (FIDO) Alliance** is opgericht om standaarden te stellen voor zowel 2FA/MFA als wachtwoordvrije authenticatie.

FIDO Universal Second Factor (U2F) is een open standaard, die specificaties voor 2FA definieert met behulp van een robuuste en fraudebestendige wachtwoordloze tweede factor. Omdat het gestandaardiseerd is, heeft FIDO U2F een brede compatibiliteit met populaire online diensten, waaronder Gmail, Facebook, Github, Dropbox en vele andere.

Biometrische vingerafdruk en hardwaresleutels die gebruik maken van USB-, NFC- of Bluetooth-technologieën zijn de typische aanvullende factoren voor diensten die gebruik maken van U2F.

VeriMark™ - de 1e Vingerafdrukbeveiligingssleutel van Kensington die zorgt voor een sterke, gestroomlijnde 2FA

VeriMark™ werkt met zowel Windows Hello als FIDO U2F authenticatie om een veilige en naadloze manier te bieden om in te loggen op Windows 7, 8.1 en Windows 10 en om 2FA in te schakelen op belangrijke accounts.

De VeriMark™ Fingerprint Key biedt de beste biometrische prestaties in zijn klasse binnen een praktisch, compact en normconform pakket.

Valse afwijzingen (3%) en valse acceptatie (0,002%) die de industriestandaarden overtreffen door gebruik te maken van TLS1.2/AES256-codering en ASP-technologie (Anti-Spoofing Protection).

VeriMark™ is de perfecte oplossing voor personen die biometrische authenticatie nodig hebben die werkt met huidige of oudere Windows besturingssystemen, terwijl het ook U2F-authenticatie ondersteunt voor cloud-gebaseerde service en software-aanbieders zoals Facebook, Google, GitHub, Dropbox en nog veel meer.

Kensington VeriMark™ Fingerprint Key

- **De geavanceerde vingerafdruktechnologie** wordt gecombineerd met uitmuntende biometrische prestaties en 360° leesbaarheid met anti-spoofingtechnologie en voldoet ruimschoots aan de industriestandaard voor False Rejection Rate (3%) en False Acceptance Rate (0,002%).
- **Universele integratie** biedt schaalbare, inventieve toegang tot Windows-computers en platforms, waaronder biometrische login voor Windows Hello™.
- **FIDO U2F gecertificeerd** voor probleemloze interoperabiliteit en voldoet aan aanmeldingsvereisten voor beveiligingssleutels voor twee-factor authenticatie voor clouddiensten en software providers die met een cloud werken, onder wie Google, Dropbox, GitHub en Facebook.
- **Dankzij een compact** ontwerp eenvoudig te bevestigen aan een sleutelhanger en gemakkelijk mee te nemen.

Onderdeelnr. K67977WW

Voor meer informatie, proefexemplaren of dealprijzen:


www.kensington.com/forget-your-password


contact@kensington.com

Bronnen

1. Risk Based Security's Q3 2019 Data Breach QuickView Report
2. darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875
3. Verizon 2019 Data Breach Investigations Report
4. securitymagazine.com/articles/88475-average-business-user-has-191-passwords
5. symantec.com/content/en/uk/enterprise/other_resources/b-is-your-data-safe-security-non-compliance-infographic-21330416-UK.pdf
6. infosecurity-magazine.com/opinions/how-much-passwords-cost
7. plan-net.co.uk/blog/password-reset-processes

FIDO® is een handelsmerk (geregistreerd in tal van landen) van FIDO Alliance, Inc.