

# Is uw bedrijf hybride veilig?

Na een verschuiving naar werken op afstand in de afgelopen jaren, ziet de toekomst er voor veel organisaties hybride uit.

Ondanks de voordelen van dit flexibele model kan het vrije verkeer tussen huis en kantoor echter aanzienlijke veiligheidsrisico's vormen.

**Volg onze eenvoudige stappen om uw bedrijf en werknemers te helpen altijd veilig en compliant te blijven in een hybride werkwereld.**

## VAN HUIS NAAR KANTOOR



# 55%

van de organisaties over de hele wereld biedt mogelijkheden voor werken op afstand. <sup>1</sup>Zorg ervoor dat u uw beleid voor hybride werken hebt aangepast om verwarring te voorkomen en risico's te verminderen.

## VERTROUWELIJKE INFORMATIE



# 88%

van de thuiswerkers heeft te maken met vertrouwelijke informatie. <sup>2</sup>Zorg ervoor dat alle vertrouwelijke bestanden, die niet langer nodig zijn, regelmatig en veilig worden vernietigd.

## SHRED-IT ALL BELEID



# 40%

40% van de datalekken wereldwijd vindt plaats als gevolg van nalatigheid van werknemers. <sup>3</sup>Een Shred-it All-beleid helpt ervoor te zorgen dat de documenten die u niet langer nodig hebt, veilig worden vernietigd, waardoor gegevenslekken worden voorkomen.

## KOSTEN VAN HYBRIDE WERKEN



# 97%

van de ondervraagde bedrijven kocht nieuwe laptops vanwege hybride werken. <sup>5</sup>Bescherm gegevens op oude en ongebruikte apparaten door harde schijven veilig te versnipperen.

## ONDERWIJS EN BEWUSTMAKING OP HET GEBIED VAN CYBERBEVEILIGING



# 39%

van de Europese bedrijven meldde in 2021 last te hebben van een cyberaanval. <sup>4</sup>Wees je bewust van cybercriminaliteit: versleutel gegevens, beperk de toegang tot vertrouwelijke informatie en verwijder de toegangsrechten van een werknemer wanneer deze het bedrijf verlaat.

1: Earth Web, 2022  
2: Shred-it Data On File, 2022  
3: Tech Republic, 2018  
4: Statista, 2021  
5: Blancco, 2020