**Categorie:** Cloud Security Innovator / **Motivatie:** The Human Centric Security standard

**De Human Centric Security standaard**

Uit gegevens van Proofpoint blijkt dat bijna alle organisaties (96%) doelwit waren van een cloud account takeover en meer dan de helft heeft dit daadwerkelijk ervaren. De helft van alle gehackte accounts had multi-factor authenticatie (MFA) ingeschakeld. Dit toont aan hoe onbeveiligde applicaties, zowel enterprise- als shadow-applicaties, waardevolle ingangen vormen voor aanvallers om de cloudaccounts van bedrijven over te nemen.

In 2024 stelt cybersecuritybedrijf Proofpoint een nieuwe security standaard in waarbij de mens centraal staat. Het bedrijf voorziet klanten van brede, adaptieve human centric securitycontroles. Het beschermt organisaties tegen dreigingen in messaging-, samenwerkings- en social media-applicaties. Ook beveiligt het SaaS-applicaties en identiteitsposities in een groot aantal toepassingen. Er wordt ook gedacht aan Data Loss Prevention (DLP), namelijk met een slimmere, flexibelere datasecurity. De adaptieve, educatieve securitybegeleiding stuurt daarnaast veiliger gedrag aan bij medewerkers. Dit alles bij elkaar vormt de nieuwe standaard voor hoe organisaties menselijke risico’s aanpakken.

Er worden twee platformelementen gebruikt voor het tackelen van menselijke risico’s, namelijk:

* [Proofpoint Nexus](https://www.proofpoint.com/us/platform/nexus), een dreigingsdetectie dat risico’s identificeert en beperkt.
* [Proofpoint Zen](http://www.proofpoint.com/us/platform/zen), een set technologieën die uitgebreide bescherming bieden terwijl mensen werken met e-mail, samenwerkingsapplicaties, internet en data.

Deze oplossingen bieden samen een geïntegreerde, samenhangende ervaring die zowel eindgebruikers als securityprofessionals een human centric-bescherming biedt.

**Proofpoint Nexus:**

* Een alles omvattend threat intelligence platform waarbij human centric security centraal staat.
* AI/ML drijven Proofpoint Nexus aan.
* Het brengt de verspreiding van user identity en veelvoorkomende aanvalsmethoden in kaart.
* Het detecteert afwijkingen in configuratie en de toegang ter voorkoming van cloud account takeover. Dit ondersteunt securityprofessionals bij het begrijpen waar een account zich bevindt. Ook helpt het bij het snappen of het risico’s oplevert vanwege de privileges, de gekoppelde data en hoe goed (of slecht) de security geconfigureerd is. Proofpoint’s Posture Management doet, op basis van houding en het risico van een identiteit, aanbevelingen en voert configuraties uit met als doel dit te verbeteren.

**Proofpoint Zen**

Proofpoint Zen gaat verder dan traditionele security awarenessprogramma’s. De technologie voedt oplossingen die risico’s in heel het digitale ecosysteem identificeren en beperken. Het biedt daardoor extra bescherming en doet de angst voor cyberdreigingen afnemen.

Proofpoint Zen bestaat uit drie oplossingen:

* **ZenWeb**, een browserextensie die wordt aangesloten op Chromium-gebaseerde browsers via verschillende apparaten. Het beschermt gebruikers op het gebied van samenwerkingstools van tools zelf, het delen van documenten en AI-applicaties. Organisaties beschermen hiermee gebruikers tijdens werk. Ook blijven ze zo dreigingen voor.
* **Zen voor Outlook** ondersteunt organisaties op het gebied van e-maildreigingen, omdat e-mail nog steeds een primaire bron voor cyberaanvallen is. De oplossing helpt het bij het herkennen, rapporteren en stoppen van dreigingen nog voordat ze schade aanrichten. Daarnaast biedt Zen voor Outlook doordachte interventies die gebruikers en data beschermen. Het beveiligt communicatiekanalen en slimme interventies zorgen ervoor dat menselijke fouten worden voorkomen. Ook stelt het gevoelige informatie veilig.
* **De ZenConnectors** integreren eenvoudig met Microsoft 365 en andere kritieke applicaties. Hierdoor breidt de securitydekking uit naar de volledige digitale workspace, waardoor security overal werkt zoals op kantoor, thuis of in een openbare werkruimte. Doordat het eenvoudig implementeert met applicaties, blijven efficiënte workflows en productiviteit behouden.