# Dutch IT Channel Awards 2026

**Data & AI Innovator of the Year: Trend Micro**
Trend Micro heeft de manier waarop organisaties zich verdedigen tegen dreigingen fundamenteel veranderd. Met **Trend Cybertron** introduceert het bedrijf zijn eerste proactieve cybersecurity-AI: technologie die dreigingen voorspelt en neutraliseert nog voordat er schade kan ontstaan. Deze innovatie is gebouwd op jarenlange AI-investeringen en 35 jaar wereldwijde threat intelligence.

**Nieuwe generatie AI**
Trend Cybertron is een gespecialiseerd cybersecurity Large Language Model, ontwikkeld voor dreigingsanalyse en -preventie. Het platform combineert dreigingsspecifieke intelligence, geavanceerde machine learning en natuurlijke taalverwerking met agentic AI-capaciteiten. Hierdoor kan het zowel dreigingen detecteren als zelfstandig analyseren, prioriteren en blokkeren.

Belangrijke onderscheidende factoren van Trend Cybertron zijn:

- **Zijn voorspellende kracht:** het voorspelt aanvalspaden op basis van organisatiecontext, kent realtime risicoscores toe en voorkomt aanvallen zoals AI-gegenereerde phishing en deepfakes. Tegelijkertijd beschermen de AI Scanner en AI Guard de AI-infrastructuur door modellen en API's te monitoren op kwetsbaarheden en afwijkend gedrag.

- **Agentic SIEM:** Trend Micro Agentic SIEM is een door AI aangedreven beveiligingsoplossing die dreigingsdetectie automatiseert, alert-moeheid vermindert en meer dan 900 databronnen integreert voor snelle, proactieve bescherming—waardoor handmatige tussenkomst door beveiligingsteams tot een minimum wordt beperkt.
- **Unieke data-architectuur:** Cybertron verwerkt gegevens uit meer dan 150 detectiemodellen, miljarden sensoren en gedragsdata van wereldwijde gebruikers, apparaten en infrastructuur. Door deze datastromen in realtime te analyseren, kunnen patronen worden herkend en dreigingen worden voorspeld. De AI-chatbot, **Trend Companion**, vertaalt deze analyses naar begrijpelijke taal, waardoor predictive security toegankelijk wordt voor elke organisatie.

**Een meetbare impact**
De resultaten spreken voor zich: organisaties die Trend Cybertron gebruiken zien 67% minder false positives, 80% snellere incidentrespons en 90% hogere nauwkeurigheid van detecties. Door meerdere losse tools te vervangen door één AI-platform realiseren klanten aanzienlijke kostenbesparingen en meer operationele efficiëntie.

Aankomende innovaties in de roadmap zijn quantum-safe algoritmen, explainable AI, federated learning en governance tools voor verantwoord AI-gebruik. Zo blijft Trend Micro continu innoveren.

**Security voor AI & samenwerking met NVIDIA**

In een tijd waarin kunstmatige intelligentie zich snel verspreidt over cloud-, core- en edge-omgevingen, wordt security voor AI een absolute noodzaak. AI-fabrieken, als nieuwe infrastructuur voor AI-workloads, brengen unieke beveiligingsuitdagingen met zich mee die traditionele beveiligingsoplossingen niet kunnen bieden. Trend Micro heeft in nauwe samenwerking met NVIDIA naast de bestaande oplossingen zoals bescherming voor NIM Microservices en integratie met NVIDIA NeMo Guardrails nu ook een baanbrekende, geïntegreerde beveiligingsoplossing ontwikkeld: Trend Vision One™ AI Factory EDR, gebouwd op NVIDIA BlueField DPUs.

Deze innovatieve samenwerking combineert geavanceerde hardwareversnelling, realtime zichtbaarheid en geavanceerde threat intelligence met krachtige Endpoint Detection and Response (EDR). Hierdoor biedt het platform realtime bescherming op schaal, zonder dat dit ten koste gaat van de AI-prestaties. Het stelt organisaties in staat om hun meest waardevolle activa — data, AI-modellen en intellectueel eigendom — optimaal te beschermen terwijl ze blijven innoveren en opschalen.

Met embedded EDR binnen de AI-infrastructuur krijgen beveiligingsteams een holistisch overzicht van elke node en workload, kunnen ze bedreigingen in realtime detecteren en voorkomen, en reageren ze sneller en gerichter op geavanceerde cyberaanvallen. Deze geïntegreerde aanpak met NVIDIA BlueField en Trend Vision One zet een nieuwe standaard voor de beveiliging van AI-infrastructuren wereldwijd, en onderstreept het leiderschap van Trend Micro en NVIDIA in het veilig mogelijk maken van AI-innovatie.

**Praktijkvoorbeelden - wat klanten zeggen**

- **Onderlinge ‘s-Gravenhage:** zet AI in om verdachte inlogpatronen automatisch te detecteren en cloudrisico’s te beoordelen. Deze aanpak verhoogt de digitale weerbaarheid aanzienlijk, zonder dat beveiligingsteams extra worden belast of operationele processen vertraagd. [lees hier de volledige klantcase]
- **Sligro Food Group:** versterke zijn supply chain- en netwerkbeveiliging met AI-gedreven dreigingsdetectie. Dankzij continue monitoring en proactief risicobeheer wordt security een strategische enabler, waardoor innovatie en marktleiderschap hand in hand kunnen gaan. [lees hier de volledige klantcase]
- **Exxaro:** koost voor Trend Cybertron vanwege de voorspellende AI-capaciteiten. Exxaro detecteert dreigingen nu sneller, reageert proactief en consolideert meerdere beveiligingsoplossingen in één platform. Dit zorgt voor meer efficiëntie, minder operationele druk en een sterkere beveiligingspositie.
- **St. Antonius Ziekenhuis:** in dit ziekenhuis wordt AI gebruikt voor behavioral analytics en het monitoren van de OT- en IoT-omgevingen. De integratie met de Cyber Risk Index zorgt voor gerichte prioritering van risico’s en een efficiënte inzet van een klein, gespecialiseerd beveiligingsteam.