

ESET introduceert nieuwe innovaties voor Intel-aangedreven AI-PC's

Met de toenemende frequentie van cyberaanvallen en de constante opkomst van nieuwe dreigingen werken technologiebedrijven samen aan baanbrekende innovaties om deze dreigingen beter te voorkomen, te detecteren en af te weren.

ESET en Intel hebben een lange geschiedenis van samenwerking op het gebied van cybersecurity. ESET is nu klaar om nieuwe functies te lanceren die gebruikmaken van Intel's nieuwste hardware-gebaseerde verdedigingsmechanismen. Deze verbeteringen zullen de efficiëntie van moderne endpointbeveiliging verder vergroten en incidentdetectie in gezamenlijke klantomgevingen versnellen.

Versnellen van cybersecurity-workloads op Intel-aangedreven AI-PC's

Hoewel de behoefte aan geavanceerde, AI-gedreven dreigingsdetectie dagelijks groeit, moeten IT-leiders rekening houden met de balans tussen de resources die nodig zijn voor cybersecuritysystemen en de prestatie- en productiviteitseisen van hybride- en externe werkscenario's. Hardwareleveranciers bieden daarom AI-PC's aan, uitgerust met niet alleen een CPU en GPU, maar ook Neural Processing Units (NPU's), die geoptimaliseerd zijn voor specifieke workloads.

Endpointbeveiligingstools moeten deze uitgebreide rekenkracht benutten om bescherming te verbeteren zonder de systeemprestaties te belasten. Om klanten te laten profiteren van deze verbeteringen in snelheid en efficiëntie, optimaliseert ESET zijn eindpuntproducten om alle beschikbare verwerkingsbronnen maximaal te benutten. Zo kan ESET's endpointbeveiligingssoftware op Intel® Core™ Ultra-gebaseerde PC's rekenintensieve taken automatisch overdragen van de CPU naar de geïntegreerde GPU of NPU. Dit laat de CPU vrij voor bedrijfskritische en prestatie-intensieve taken zoals videoconferencing en data-analyse en verbetert de systeemefficiëntie.

Verbeterde prestaties en efficiëntie met NPU-computing

ESET zet een evolutionaire stap door gebruik te maken van de voordelen van de NPU binnen Intel's Core Ultra-processorarchitectuur. Deze technologie verdeelt AI-workloads in ESET's endpoint producten over de NPU. Een belangrijk gebruikvoorbeeld is het uitvoeren van neurale netwerkmodellen binnen de op machine learning gebaseerde modules van ESET.

Door deze workloads naar de GPU of NPU binnen de Intel Core Ultra-processor te verplaatsen, wordt het energieverbruik verbeterd zonder concessies te doen aan de prestaties. Dit verhoogt de schaal van de neurale modelberekeningen, wat de veerkracht van endpoints van klanten versterkt zonder negatieve invloed op efficiëntie of prestaties. Voor zware taken zoals AI- of ML-berekeningen kan de NPU worden ingezet, wat de detectietijd vermindert en de efficiëntie verhoogt.

Deze verbeteringen worden steeds waardevoller, bijvoorbeeld bij lokaal intensieve of gevoelige workloadverwerking, of wanneer de beveiliging wordt versterkt bij toegang tot cloudgebaseerde AI-resources.

“Een win-winsituatie”

Előd Kironský, Vice President van Endpoint Solutions and Security Technologies bij ESET, stelt: *“Deze vroege winst laat onze toewijding zien aan het ontwikkelen van producten met*

een lage systeembelasting, een gebied waarin ESET altijd heeft uitgeblonken. Het benutten van technologie binnen Intel-aangedreven AI-PC-architectuur voor zowel preventie als bescherming, terwijl prestaties behouden blijven, is een win-winsituatie.”

Gebruik van Intel's hybride architectuur

De gezamenlijke inspanningen van ESET en Intel op het gebied van AI-PC's worden ondersteund door recente optimalisaties in ESET Endpoint-beveiligingssoftware, die profiteren van Intel's nieuwste hybride processorarchitectuur. Met bewustzijn van hybride cores – prestatie- en efficiëntiekernen – kunnen workloads worden toegewezen aan de meest geschikte kern, afhankelijk van de taak.

Volgens Kironský: “Het toewijzen van workloads aan efficiënte kernen heeft geen negatieve impact op de productprestaties, en prestatieverbeteringen zijn in verschillende scenario's aangetoond. Zo kunnen we diepgaande bescherming bieden zonder kritieke processen te verstoren.”

Toekomstige mogelijkheden voor AI-PC's

Het onderzoek naar AI-PC-architecturen is slechts één van de gebieden waarin ESET en Intel samenwerken om cybersecurity en gebruikerservaring te verbeteren. Mogelijkheden omvatten:

- Het creëren van kleine neurale netwerkmodellen voor specifieke malwarefamilies, voor snellere- en consistentere detectie.
- Beeldherkenning via neurale netwerken om phishing en andere scams te identificeren.
- Gebruik van grote taalmodellen (LLM's) om incidentdetecties op endpoints te beschrijven en forensische analyses te verbeteren.

De toekomst van cybersecurity hervormen

De voortdurende samenwerking tussen ESET en Intel benadrukt de noodzaak om verder te gaan dan incrementele productverbeteringen en substantiële sprongen te maken die het dreigingslandschap hervormen. De toekomst van endpointbeveiliging ligt in een geïntegreerde aanpak van hardware- en softwaretechnologieën die AI-computerbronnen omarmen en hybride werk ondersteunen.

ESET blijft innoveren met Intel voor toekomstige generaties processors die AI-PC's aandrijven. Deze gedeelde innovatieruimte, waarin CPU, GPU en NPU samenkomen, beschermt bedrijven tegen bekende en onbekende dreigingen en borgt een toekomstbestendige interface tussen software- en hardwaregebaseerde beveiligingstechnologieën.

De nieuwe functies zoals NPU- en GPU-offload zijn beschikbaar in ESET's Endpoint-productlijn sinds december 2024.