Case Study

intel

Intel und VNClagoon – Intelligente Prozessortechnologie für die sichere und schnelle Anwendung generativer KI

Die Herausforderung: Die meisten generativen KI-Modelle arbeiten in großen Cloud-Umgebungen, was sie anfällig für Angriffe macht. Wir bieten Ihnen eine echte Alternative. Setzen Sie die KI-Algorithmen auf Ihren eigenen Systemen ein, integrieren Sie sicher Ihre Daten und erreichen Sie die beste Performance – auf einer Deep-State-Verschlüsselungs- und Hardware-Ebene, unter Verwendung Ihrer eigenen PCs und Ihrer eigenen Rechenzentren.

Erfahren Sie mehr über diese Zusammenarbeit zwischen Intel und VNClagoon.

Generative KI verändert die Art und Weise, wie die Welt funktioniert

– sie macht uns noch stärker abhängig von Daten als Treibstoff für den Erfolg im geschäftlichen Umfeld.

Generative KI verspricht ein exponentielles Wachstum bei der Lösung vieler Herausforderungen.

Doch die KI stellt hohe Anforderungen an die zugrunde liegenden Rechenkapazitäten:

- Unternehmen des öffentlichen Sektors wollen Verwaltungsprozesse mit Millionen von unterschiedlichen Datenpunkten rationalisieren
- Banken analysieren Tausende Transaktionen in Echtzeit, um Betrug zu verhindern
- Konsumgüterunternehmen wollen Millionen von Kunden mit individuellen Botschaften ansprechen

In einer datengetriebenen Welt sind Aufgaben, die vor einigen Jahren noch unlösbar waren, plötzlich machbar. Doch der Einsatz von GenAI birgt mit dem hohen Datenbedarf auch Risiken: Denn um optimale Ergebnisse zu erzielen, müssen Unternehmen sensible Unternehmens- und Kundendaten weitergeben.

Vor allem für Unternehmen, die ihre internen Daten schützen wollen, aber dennoch von den neuesten KI-Fortschritten profitieren möchten, ist es an der Zeit, die Technologie in einer sicheren und geschützten Sandbox-Umgebung auszuführen. Willkommen, VNClagoon!

Wer ist VNC?

VNC (VNC - Virtual Network Consult AG) ist ein globales Softwareunternehmen mit Sitz in der Schweiz, das Open-Source-basierte Kommunikations- und Kollaborationsanwendungen entwickelt. Mit VNClagoon bietet das Unternehmen eine spezialisierte Suite für sichere Kommunikation und kollaboratives Arbeiten.

Die größte Stärke dieser Lösung ist, dass VNClagoon vollständig auf Open-Source-Technologie basiert und dabei in eine sichere Cloud-Umgebung integriert ist.

VNClagoon folgt einer modularen Architektur und bietet eine sichere, einheitliche Kommunikations- und Kollaborationssuite mit vielen Funktionen:

- Groupware (E-Mail-Einrichtung, Kalenderfunktionen)
- Chat und Videokonferenzen
- CRM
- Aufgaben- und Projektverwaltung
- Dateiverwaltung
- Dateiverzeichnisse
- Dashboards

Alle diese Funktionen sind mit einem **integrierten generativen KI-Agenten ausgestattet, der die Produktivität steigert und mit Intels neuester Prozessortechnologie betrieben wird.**

Dies macht VNClagoon zu einer idealen Lösung für große Unternehmen im Gesundheitswesen, im öffentlichen Sektor und im Finanzdienstleistungssektor, die mit sensiblen Daten arbeiten.

Erfahren Sie hier mehr: www.vnclagoon.com

Confidential AI mit Intel Technologies –

Wir haben die perfekte Lösung für Ihre GenAI-Herausforderungen gefunden!

Wir nutzen das Beste aus beiden Welten – Intels neueste High-End-Prozessoren – und VNClagoons sichere Cloud-Umgebung und bieten Ihnen erstklassige Leistung und erhöhte Sicherheitsstandards. Die bereitgestellte Lösung nutzt das Intel OpenVINO™-Toolkit, das die Inferenzlatenz deutlich reduziert und somit die Ausführungsgeschwindigkeit signifikant verbessert, während die Qualität der Ergebnisse kontinuierlich hoch bleibt – in der Cloud oder auf Ihrem Endgerät.

In Kombination mit der Privacy Suite von VNClagoon ermöglicht Intel Ihnen die sichere Ausführung von GenAI-Algorithmen, insbesondere von großen Sprachmodellen (LLMs), in einer sicheren Sandbox-Umgebung.

Durch diese Zusammenarbeit sind GenAI-Anwendungen von den Plattformen der großen KI-Lösungsanbieter entkoppelt – somit wird jeglicher unbefugter Zugriff verhindert. Das System funktioniert am besten auf PCs mit der neuesten Generation von Intel® Core™ Ultra Prozessoren, auf denen Sie von einer verbesserten generativen KI-Leistung und Energieeffizienz profitieren.

Behalten Sie die Kontrolle über Ihre Trainingsdaten – überall und zu jeder Zeit

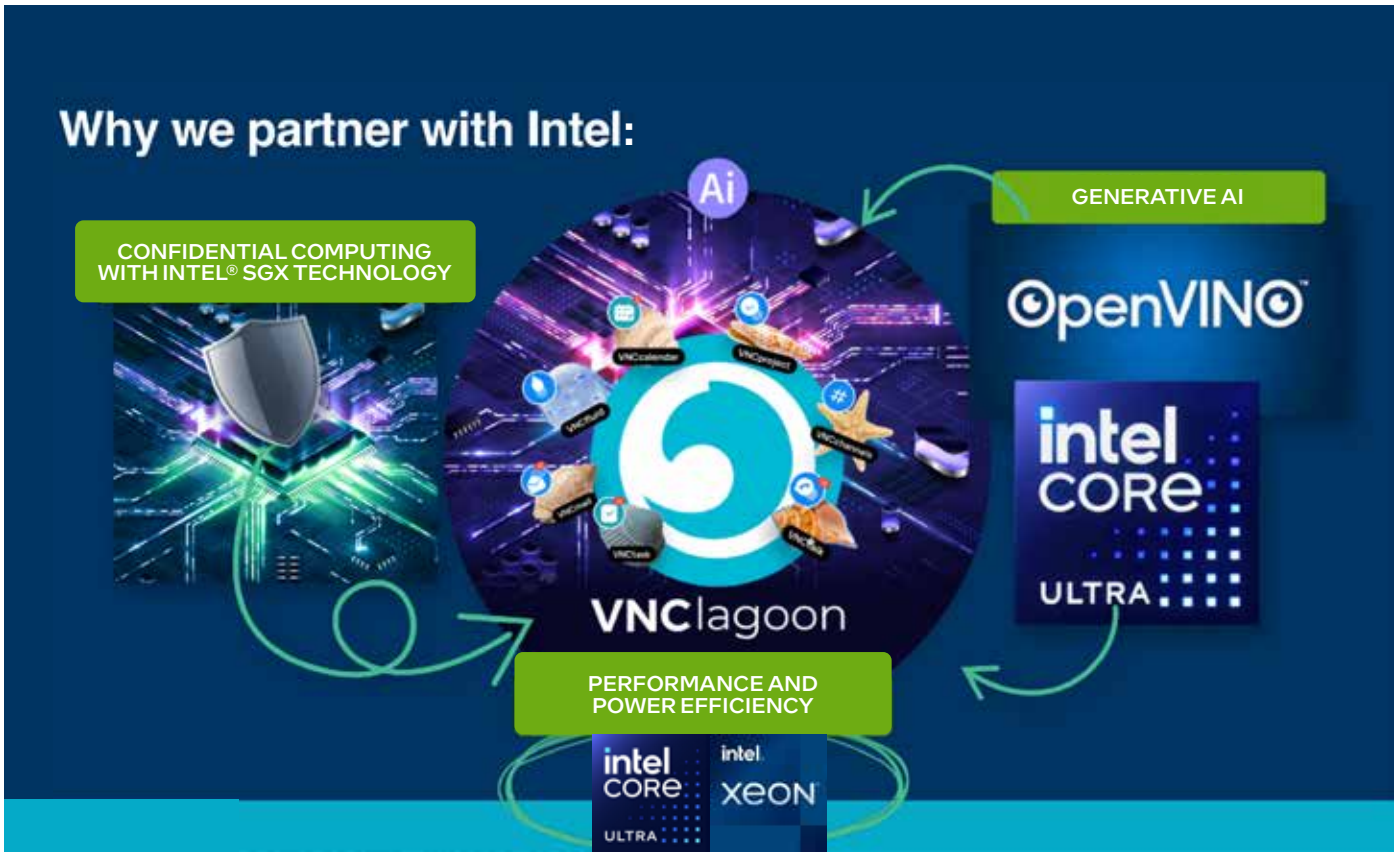
Mit dem Intel OpenVINO-Toolkit können Sie KI-Algorithmen innerhalb der VNClagoon-Umgebung einsetzen. Alle Trainingsdaten der generativen KI können dabei sicher ausgeführt und mit jeder Iteration kontinuierlich verbessert werden. Viele LLMs stützen sich auf ähnliche Frameworks, aber durch die Ausführung mit Intel OpenVINO können Sie die Runtime stark beschleunigen. Das Toolkit verbessert die Inferenzlatenz eines KI-Modells und ermöglicht rasante Ausführungen in sicheren Cloud-Umgebungen.

Machen Sie das Beste aus Ihrer Privatsphäre

Suchen Sie ein sicheres Framework für den Zugriff und die sichere Verarbeitung von Daten? VNClagoon bietet Ihnen eine geschützte Sandbox-Umgebung, in der Sie Ihre Daten speichern, zusammenführen und aktualisieren können. Die Suite minimiert die Gefahr eines unbefugten Zugriffs oder einer Verletzung des Datenschutzes erheblich. Angetrieben von einer Intel® Xeon®-basierten Cloud-Infrastruktur (mit Intel SGX) und dem Zugriff von einem PC, der auf der Intel-Meteor-Lake-Architektur basiert, können wir Ihnen ein Höchstmaß an Datenschutz und Sicherheit garantieren.

Meisten Sie KI-Compliance

Regulierungsbehörden stellen hohe Anforderungen an die Datensicherheit, und künftige Verordnungen (z. B. das KI-Gesetz der Europäischen Union) könnten Fortschritte in der KI-Technologie innerhalb Ihres Software-Stacks behindern. Die Zusammenarbeit zwischen VNClagoon und Intel verschafft Ihnen einen Vorsprung im Umgang mit sensiblen Kundendaten und macht Ihren Software-Stack zukunftssicher.



Technische Details zu Intel OpenVINO™

(Open Visual Inference and Neural Network Optimization)

Die Intel OpenVINO™ Technologie ist für ressourcenarme Umgebungen optimiert. Sie läuft auf durchgängig sicheren Geräten unter Verwendung von Laptops mit den neuesten Intel® Core™ Ultra Meteor Lake Chips, reduziert aber auch die Latenz, wenn auf einen KI-Agenten aus einer Cloud-Umgebung zugegriffen wird.

- OpenVINO ermöglicht es Ihnen, vortrainierte KI-Algorithmen auf kleinere Modelle mit einem festen Satz von Trainingsdaten abzubilden. Es verwendet einen Modell-Optimierer, der Sie beim Übergang zwischen einer Trainings- und einer Deployment-Umgebung unterstützt.
- OpenVINO läuft flexibel auf verschiedenen Hardwarekonfigurationen (auf GPUs, CPUs und NPs; vor Ort und auf Geräten; im Browser oder in der Cloud)
- Mit der statischen Modellanalyse von OpenVINO können Sie die Geschwindigkeit für beliebige generative KI-Anwendungen erheblich steigern
- OpenVINO optimiert die bestehenden Modelle und konvertiert sie in eine intermediäre Darstellung (einschließlich XML-Beschreibungen, .bin-Datei mit „Gewichten“ und Binärdaten). In späteren Phasen werden sie an eine Inferenz-Engine weitergeleitet, durch die Sie die Algorithmen auf Grundlage des gewählten Zielgeräts weiter optimieren können.
- **Dieser Prozess reduziert die Größe eines GenAI-Modells im Durchschnitt um etwa 50 Prozent!** Dadurch wird auch der Laufzeitspeicher während des Compilings reduziert, sodass die Algorithmen auf Edge-Systemen statt in großen Rechenzentren ausgeführt werden können.

Secure Cloud - Schützen Sie Ihre Daten mit Intel Computing

Intel® Xeon® ist eine skalierbare Prozessorarchitektur, die sich ideal für große Rechenzentren eignet und eine Cloud-Architektur bietet, mit der sich LLMs (wie das in VNClagoon integrierte) ausführen lassen.

Um Confidential Computing umzusetzen, sind die Intel® Xeon® CPUs bereits mit Intel SGX (Software Guard Extensions) und Intel TDX (Trust Domain Extension) ausgestattet. Beide Technologien schaffen eine vertrauenswürdige Ausführungsumgebung (Trusted Execution Environment, TEE), die einige entscheidende Vorteile für generative KI-Technologie bietet:

- Confidential Computing funktioniert direkt auf der Hardware-Ebene. Datenprozesse, die mit Intel SGX ausgeführt werden, können dabei eine Prozesstrennung über verschiedene Enklaven nutzen, sodass sie von externem Code nicht ausgelesen werden können (auch nicht von höherprivilegiertem Code, wie z. B. Betriebssystemcode und anderer Hardware-Infrastruktur), während Intel TDX eine vollständige virtuelle Maschine innerhalb der TEE bereitstellt, die Betreiber und Workload-Owner voneinander trennen.
- Beide Technologien ermöglichen konsistente Audits und Hardware-Sicherheitsupdates auf Ihren Servern. Vor jedem Datenaustausch zwischen verschiedenen Systemteilen gibt es einen Bestätigungsmechanismus (kryptografische Überprüfung, dass das TEE echt und wie erwartet konfiguriert ist), sodass Sie sicher sein können, dass Ihre Anwendungen nicht kompromittiert worden sind.
- Durch diese mehrstufigen Sicherheitsebenen sind Ihre Daten im Server-Backend sowie der Datenfluss zu Ihren clientbasierten generativen KI-Modellen immer gesichert!

Die nächste Stufe des generativen-KI-Computings wartet auf Sie!

VNClagoon (in Kombination mit Intel OpenVINO™ und Intel Confidential Computing) ist die perfekte Lösung, um Ihre geschäftsinterne Kommunikation und Kollaboration zu optimieren. Neben erhöhter Sicherheit bei der Anwendung generativer KI bieten wir Ihnen eine Reihe von wichtigen Vorteilen:

- Echtzeit- Indexierung von Inhalten aus jedem VNClagoon-Produkt auf Basis von Apache Solr für eine intelligente Suche und für den Einsatz von Chatbots
- Multi-Device-Frontend (einschließlich Edge-Computing auf Endnutzergeräten)
- Aktuelle Integration von Metas Llama in VNClagoon (zudem werden acht weitere KI-Modelle in Kürze folgen). Die Zusammenarbeit ermöglicht den sicheren Betrieb der LLMs auf Ihren eigenen Systemen und schützt Ihre Daten, die zum Training der LLMs verwendet wurden, sowie den Code der proprietären Modelle

Gemeinsam helfen Intel und VNClagoon Ihnen, das Beste aus Ihrer Hardware-Infrastruktur herauszuholen! Kontaktieren Sie einfach unsere Experten oder wenden Sie sich an Ihre bevorzugten Intel-Händler oder Integratoren, um Ihr eigenes VNClagoon mit Intel® Core™ Ultra Meteor Lake Prozessoren unter Verwendung von Intel OpenVINO™ einzurichten. Profitieren Sie zudem von den Backend-Services, die von Intel ® Xeon ™-Prozessoren angetrieben und von Intel SGX und Intel TDX geschützt werden.

Erfahren Sie mehr und sehen Sie sich die vollständige Demo hier an: Neues VNClagoon AI Demo Video - VNClagoon

Kundenreferenz

VNClagoon basiert auf Open-Source-Technologie und nutzt Intel Confidential Computing. Die Lösung wird beständig weiterentwickelt und derzeit als sicheres KI-Frontend für das **von Fujitsu geleitete Projekt eArchive4Future** eingeführt. Dieses Projekt soll dem größten Dokumentenarchiv des öffentlichen Sektors in Deutschland, das von der Bundesagentur für Arbeit genutzt wird, einen langfristigen technologischen Weg in die Zukunft ebnen.