GECCO et enclaive apportent l'informatique confidentielle et le chiffrement post-quantique aux déploiements edge

Protéger les données en cours d'utilisation dans les environnements critiques, souverains et intégrant l'IA.

VICTORIA, CANADA, September 14, 2026 /EINPresswire.com/ -- Green Edge Computing Corp. (GECCO) et le leader du chiffrement 3D, enclaive, basé en Allemagne, annoncent un partenariat stratégique : la brique logicielle d'informatique confidentielle (confidential computing) et de chiffrement d'enclaive sera intégrée à l'EdgePod, l'appliance de calcul et stockage durcie à trés basse consommation de GECCO.

> “Avec GECCO, nous apportons le chiffrement en cours d'utilisation, le contrôle d'accès piloté par attestation et des services de confiance post-quantiques dans les environnements edge.”
>
> *Andreas Walbrodt*

Objectif: rendre l'informatique confidentielle, prête pour l'ère post-quantique, disponible dans les déploiements edge distribués. Gouvernements, entreprises, acteurs de la santé, opérateurs télécoms et exploitants d'infrastructures critiques pourront ainsi traiter leurs données sensibles en toute sécurité, au plus près du terrain.

Hôpitaux, sous-stations électriques, sites de défense, installations industrielles et autres segments: les organisations qui exploitent des opérations critiques sont des cibles privilégiées, pour des attaquants externes comme pour des menaces internes. Or le chiffrement conventionnel ne protège que les données stockées (au repos) et celles qui circulent sur les réseaux (en transit) ; les charges de travail sensibles restent exposées pendant leur exécution. Même lorsque ces organisations adoptent l'informatique en périphérie (edge computing), sur site ou à proximité, pour limiter leur dépendance aux réseaux et aux centres de données de prestataires tiers, la protection des données en cours d'utilisation reste un point faible.

GECCO et enclaive comblent cette lacune en associant une infrastructure edge durcie à une informatique confidentielle ancrée dans le matériel : protection des données en cours d'utilisation au sein d'environnements d'exécution de confiance (TEE), attestation à distance, identité des charges de travail (workloads) et gestion des clés contrôlée par le client.

Le GECCO EdgePod est une appliance edge durcie à très basse consommation énergétique qui permet calcul, stockage, réseau et exécution des charges de travail du lieu où les données sont produites. Conçu pour les environnements difficiles et critiques, il réduit les contraintes de taille, de poids, de puissance et de refroidissement par rapport aux infrastructures en rack

conventionnelles, et se déploie là où une salle serveur ou un centre de données n'est pas envisageable.
Les solutions d'informatique confidentielle d'enclaive apportent le chiffrement, l'attestation, l'identité et la gestion des clés nécessaires pour protéger les charges de travail sensibles pendant leur exécution. La suite comprend des machines virtuelles confidentielles, Confidential Kubernetes, la sécurisation de l'IA, la gestion des secrets et des clés fondée sur un vHSM (module de sécurité matériel virtuel), la gestion des identités et des accès des charges de travail, l'attestation à distance et des fonctions de gouvernance. Ensemble, ces technologies garantissent que secrets, clés, modèles et données sensibles ne sont délivrés qu'à des charges de travail vérifiées, s'exécutant dans des environnements d'exécution de confiance.
Il en résulte une plateforme d'edge confidentiel dédiée à l'inférence IA sensible, au traitement de données et à toute charge de travail virtualisée ou conteneurisée, sous contrôle cryptographique renforcé. Plutôt que de s'en remettre à des fournisseurs de cloud centralisés ou à des périmètres de sécurité réseau classiques, la solution “Confidential Edge” de GECCO/enclaive établit la confiance au niveau de la charge de travail, vérifie l'environnement d'exécution et maintient la protection des données jusque pendant leur traitement.
« En déployant la solution de “confidential computing” d'enclaive sur l’équipement edge durci de GECCO, nous offrons un niveau de sécurité inédit pour les déploiements critiques en périphérie. Une infrastructure basse consommation, déployable partout, associée au chiffrement en cours d'utilisation, à l'attestation à distance et à la gestion des clés contrôlée par le client : c'est ce qui permet d'exécuter en toute sécurité les charges de travail les plus sensibles là où le cloud ou les systèmes en rack conventionnels ne sont pas envisageables », déclare Jeff MacMillan, Cofounder et CEO de GECCO.
Le partenariat s'adresse en priorité aux organisations qui veulent ou doivent s’assurer de leur souveraineté sur leurs données sensibles tout en opérant dans des environnements physiquement exposés ou à bande passante limitée : inférence IA sur données réglementées, analyse sécurisée de données de santé, charges de travail tactiques de défense, industrie et production manufacturière, énergie et services publics, services edge des télécoms, systèmes du secteur public et autres infrastructures critiques.
« L'informatique confidentielle change le modèle de sécurité : on ne fait plus confiance à l'infrastructure, on la vérifie. Avec GECCO, nous apportons le chiffrement en cours d'utilisation, le contrôle d'accès piloté par attestation et des services de confiance post-quantiques dans les environnements edge durcis où les données sensibles doivent, de plus en plus, être traitées », déclare Andreas Walbrodt, cofondateur et CEO d'enclaive.
La collaboration prend également en charge des flux de sécurité crypto-agiles, prêts pour la cryptographie post-quantique. Pour accompagner cette transition, l'architecture GECCO/enclaive consolide les opérations cryptographiques utilisées pour l'attestation, l'identité des charges de travail, les certificats, le provisionnement des secrets et la gestion des clés. Elle renforce la confiance opérationnelle sur les sites edge distribués grâce à une approche de sécurité globale, alliant contrôles d'accès physiques et mécanismes cryptographiques post-quantiques ou hybrides normalisés.
Rencontrez GECCO et enclaive
 ALL IN, Montréal, 16-17 septembre 2026 – https://allinevent.ai/

 it-sa Expo & Congress, Nuremberg, 27-29 octobre 2026 – https://www.itsa365.de/en/it-sa-expo-congress

À propos de Green Edge Computing Corp. (GECCO)
Green Edge Computing Corp. conçoit et fabrique des systèmes d'informatique en périphérie (edge computing) robustes et compacts pour les déploiements souverains, critiques et en environnements difficiles. Sa plateforme EdgePod réunit calcul, stockage, réseau et gestion des charges de travail dans un appareil basse consommation, conçu pour les sites où les infrastructures en rack classiques ne sont pas adaptées. GECCO sert les secteurs de la défense, de la sécurité publique, des infrastructures critiques, des télécommunications, de la santé et de l'industrie, ainsi que les communautés isolées.
Pour en savoir plus : www.g3cco.com

À propos d'enclaive
enclaive est une entreprise technologique internationale dont le siège se situe en Allemagne. Ses solutions sont déjà adoptées par une communauté solide et engagée d'éditeurs de logiciels indépendants (ISV), de fournisseurs de services gérés (MSP) et de fournisseurs de services cloud (CSP) dans le monde entier. Grâce à son approche de l'informatique confidentielle (Confidential Computing), les entreprises protègent efficacement leurs données et applications sensibles. Son système d'exploitation multi-cloud complet met en œuvre une sécurité Zero Trust en chiffrant les données jusque pendant leur utilisation et en isolant les applications à la fois de l'infrastructure et des fournisseurs de solutions. Les entreprises conservent ainsi un contrôle total sur leurs informations confidentielles.
Pour en savoir plus : www.enclaive.io

Rudi Carolsfeld
Green Edge Computing Corp (GECCO)
8553343763 ext.
contact@g3cco.com
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/942176007

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.