GECCO and enclaive bring confidential computing and post-quantum-ready encryption to rugged edge deployments

Protecting data in use for mission-critical, sovereign, and AI-enabled environments.

VICTORIA, CANADA, September 14, 2026 /EINPresswire.com/ -- Green Edge Computing Corp. (GECCO) and the German cybersecurity company enclaive have announced a strategic partnership to integrate enclaive's confidential computing and encryption software stack into GECCO's rugged, low-power EdgePod computing appliance. The collaboration is focused on enabling post-quantum-ready confidential computing for distributed edge deployments, giving governments, enterprises, healthcare providers, telecom operators, and critical infrastructure owners the ability to process sensitive data securely at the edge.

> "Working with GECCO, we can bring encryption-in-use, attestation-driven access control, and post-quantum-ready trust services into rugged edge environments where sensitive data needs to be processed."
>
> *Andreas Walbrodt*

Organizations that run critical operations like hospitals, substations, defence sites, and industrial facilities are often targeted by bad actors, both internal and external. One of the most common security gaps is that conventional encryption protects only stored data (data at rest) and data crossing networks (data in transit), while sensitive workloads remain exposed during processing. Even as these organizations move to edge computing (on-premise or near-premise) to reduce their risk of exposure to networks and data centres operated by third party providers, protecting data while being processed on the edge is an ongoing security concern. GECCO and enclaive are addressing this gap by combining rugged edge infrastructure with hardware-rooted confidential computing – the protection of data in use in trusted execution environments –, remote attestation, workload identity, and customer-controlled key management. The joint architecture brings together the strengths of both companies through two core components:

The GECCO EdgePod provides a compact, rugged, low-power edge computing appliance that brings data processing, storage, networking, and workload execution closer to where data is created. Purpose-built for harsh and mission-critical environments, the EdgePod reduces size, weight, power, and cooling demands compared with conventional rack-mounted IT infrastructure, while supporting deployment in locations where a traditional server room or data

centre is not practical.

enclaive's confidential computing solutions provide the encryption, attestation, identity, and key-management capabilities required to protect sensitive workloads during execution. enclaive's software stack includes confidential virtual machines, Confidential Kubernetes, and AI security as well as vHSM-based secret and key management, workload identity and access management, remote attestation, , and governance capabilities.
Together, these technologies are intended to ensure that secrets, keys, models, and sensitive data are released only to verified workloads running in trusted execution environments.

The result of this collaboration is a confidential-edge platform for sensitive AI inferencing, data-processing, and any virtualized or containerized workloads while maintaining strong cryptographic control. Instead of exposure to centralized cloud service providers or relying on conventional cybersecurity perimeters across networks, the GECCO/enclaive solution is designed to establish trust at the workload level, verify the execution environment, and keep data protected even during processing.

"When enclaive's confidential computing software is deployed on GECCO's rugged edge computing platform, we can offer a level of security for mission-critical edge deployments that was not possible until now. Low-power, deploy-anywhere infrastructure combined with encryption-in-use, remote attestation, and customer-controlled key management, makes it possible to securely deploy the most sensitive workloads in places where conventional cloud or rack-based systems are not practical," said Jeff MacMillan, Co-Founder and CEO at GECCO.

The partnership is especially relevant for organizations that must maintain sovereignty over sensitive data while operating in physically exposed or bandwidth-constrained environments. Potential applications include AI inference on regulated data, secure healthcare analytics, tactical defence workloads, industrial and manufacturing, energy and utility operations, telecom edge services, public-sector systems, and other critical infrastructure systems.

"Confidential computing changes the security model from trusting infrastructure to verifying it. Working with GECCO, we can bring encryption-in-use, attestation-driven access control, and post-quantum-ready trust services into rugged edge environments where sensitive data increasingly needs to be processed," said Andreas Walbrodt, Co-Founder and CEO at enclaive.

The collaboration will also support crypto-agile and post-quantum-ready security workflows. As organizations prepare for the transition to post-quantum cryptography, the GECCO/enclaive architecture consolidates cryptographic operations used across attestation, workload identity, certificates, secret provisioning, and key-management processes. This architecture supports stronger operational trust in distributed edge locations through a full-stack security approach spanning physical access controls and standardized post-quantum or hybrid cryptographic mechanisms.

Meet GECCO and enclaive at the following events:
ALL IN, Montreal, 16-17 September 2026
https://allinevent.ai/
it-sa Expo & Congress, Nuremberg, 27-29 October 2026
https://www.itsa365.de/en/it-sa-expo-congress

About Green Edge Computing Corp. (GECCO)
Green Edge Computing Corp. designs and manufactures rugged, compact edge computing systems for sovereign, mission-critical, and harsh-environment deployments. GECCO's EdgePod platform brings compute, storage, networking, and workload management into a low-power appliance designed for locations where conventional rack-mounted IT infrastructure is impractical. GECCO serves defence, public safety, critical infrastructure, telecom, healthcare, industrial, and remote-community applications. Visit www.g3cco.com.

About enclaive
enclaive is an international technology company headquartered in Germany. Its solutions already serve a strong and dedicated community of ISVs, MSPs, and CSPs around the world. Through enclaive's Confidential Computing approach, companies can securely protect their sensitive data and applications. The comprehensive multi-cloud operating system enables Zero Trust security by encrypting data even while it's in use and shielding applications from both infrastructure and solution providers. This enables companies to retain complete control over their confidential information. Learn more at www.enclaive.io

Rudi Carolsfeld
Green Edge Computing Corp (GECCO)
8553343763 ext.
email us here
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/942172423

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.