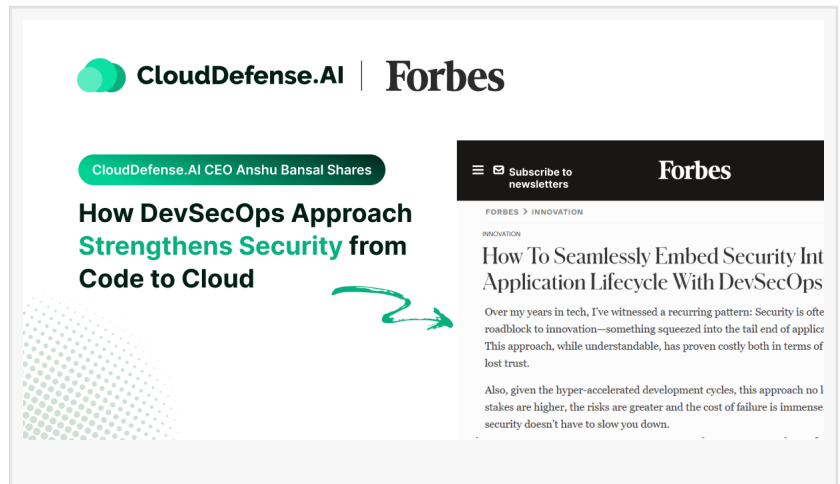# CloudDefense.AI CEO Anshu Highlights the Importance of Embedding Security into Every Stage of Application Development

PALO ALTO, CA, UNITED STATES, March 4, 2025 /EINPresswire.com/ -- CloudDefense.AI continues to drive innovation in cloud and application security with expert insights from its CEO, Anshu Bansal, who was recently featured in Forbes. In his latest article, "How to Seamlessly Embed Security Into Your Application Lifecycle with DevSecOps," Anshu explores how modern businesses can adopt a proactive security approach by

integrating security directly into their software development processes - ensuring both speed and safety in application delivery.

As businesses increasingly prioritize faster release cycles and continuous innovation, traditional security practices are no longer enough. Anshu emphasizes that treating security as a final checklist or isolated phase leaves organizations vulnerable to evolving threats. Instead, DevSecOps - the seamless integration of security into development and operations - is becoming essential for businesses aiming to build secure, resilient software without compromising agility.

> " Security isn't a gate at the end of development - it's the foundation for innovation itself."
>
> *Anshu Bansal, CEO of CloudDefense.AI*

The article breaks down the practical strategies for embedding security across the entire application lifecycle -from initial planning and development to testing, deployment, and ongoing monitoring. By making security everyone's responsibility, from developers to operations and leadership, companies can catch vulnerabilities earlier, reduce costly rework, and create a culture where security enhances innovation rather than slowing it down.

Anshu also highlights the growing need for automated security tools that fit directly into

developer workflows, ensuring that security checks happen automatically within CI/CD pipelines. By continuously monitoring for risks and aligning security policies across all stages, businesses can proactively defend their applications while keeping pace with today's rapid development demands.

For the full Forbes article, click here.

About CloudDefense.AI:

CloudDefense.AI, headquartered in Palo Alto, is a complete Cloud-Native Application Protection Platform (CNAPP) that secures the entire cloud infrastructure and applications. Considering the evolving threat landscape, they blend expertise and technology seamlessly, positioning themselves as the go-to solution for remediating security risks from code to cloud.

Experience the ultimate protection with their comprehensive suite that covers every facet of your cloud security needs, from code to cloud to cloud reconnaissance. Their catered-for cloud offering includes SAST, DAST, SCA, IaC Analysis, Advanced API Security, Container Security, CSPM, CWPP, and CIEM to the exclusive Hacker's View™ technology - CloudDefense.AI ensures airtight security at every level.

Going above and beyond, their innovative solution actively tackles zero-day threats and effectively reduces vulnerability noise by strategically applying various modern techniques. This unique approach delivers up to five times more value than other security tools, establishing them as comprehensive and proactive digital defense pioneers.

If you want to learn more about CloudDefense.AI and explore one of the best CNAPPs in the industry, please book a free demo with us or connect with us here at connectwithus@clouddefense.ai

Emily Thompson
CloudDefense.AI
media@clouddefense.ai
Visit us on social media:
X
LinkedIn
Instagram
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/790906938

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.