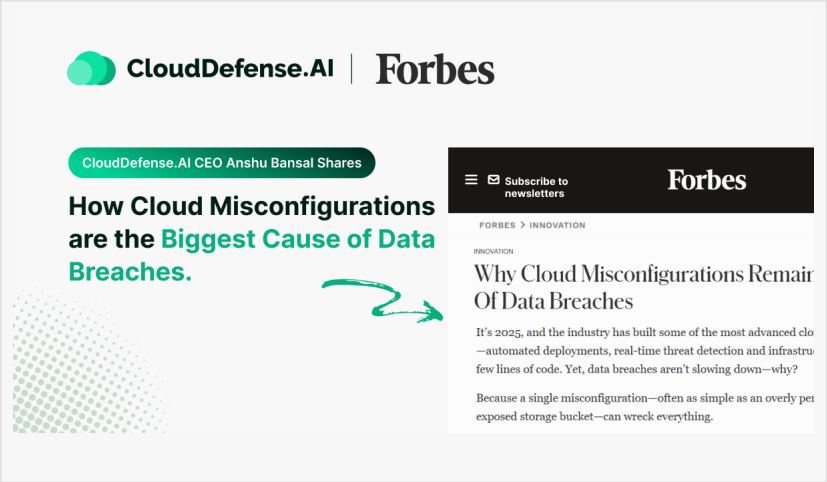
CloudDefense.AI CEO Anshu Shares How Cloud Misconfigurations are the Biggest Cause of Data Breaches



PALO ALTO, CA, UNITED STATES, April 9, 2025 /EINPresswire.com/ -- Cloud misconfigurations continue to top the list of threats in today's digital landscape, and CloudDefense.AI is leading the charge to address them head-on. In his latest Forbes feature, "Why Cloud Misconfigurations Remain A Top Cause Of Data Breaches", CEO Anshu Bansal explores how even the most advanced cloud environments are still vulnerable to simple, overlooked errors. Despite automation and real-time detection innovation, data breaches continue, often due to misconfigurations hiding in plain sight.

According to Anshu, the problem isn't just about technical oversight – it's systemic. Misconfigurations arise from the disconnect between how cloud environments are built, secured, and understood. A single misstep, such as an exposed storage bucket or overly broad IAM permissions, can have cascading effects across an organization's infrastructure.

> Misconfigurations aren't just technical glitches – they're the silent saboteurs of cloud security."
>
> *Anshu Bansal, CEO, CloudDefense.AI*

Modern development practices, like Infrastructure as Code (IaC) and rapid CI/CD pipelines, make these errors harder to catch. Developers often deploy resources quickly, and security teams don't see the changes until they're live. This gap allows misconfigurations to slip through unnoticed, putting sensitive data at risk before anyone can respond.

Anshu argues that the industry's biggest failure is not the lack of tools, but the continued focus on detection over prevention. Traditional tools raise countless alerts but often fail to provide the context to prioritize real threats. As a result, critical issues get lost in the noise while attackers exploit the gaps.

The root causes run deeper than human error. Speed often takes priority over security, and default configurations meant for convenience leave systems exposed. Configuration drift, siloed workflows, and lack of context all contribute to a security environment where vulnerabilities can persist for weeks or months.

To address these risks, Anshu emphasizes the importance of shifting security left and bringing it into the development process. Developer-friendly tools that flag risky settings early can prevent misconfigurations before deployment. Enforcing least privilege, automating policies, and continuously monitoring environments are essential to this approach.

Advanced tools like CSPM platforms that combine configuration insights with contextual risk help teams act on what matters most. A misconfigured bucket serving public logs is not as urgent as one exposing customer data – and security teams need clarity to prioritize effectively. Without that clarity, even well-resourced teams struggle to keep up.

Anshu's message is clear: fixing misconfigurations requires more than technology – it demands a cultural shift. Organizations become truly resilient when everyone from developers to executives owns cloud security.

To dive deeper into these insights, read Anshu Bansal's full article on Forbes.

About CloudDefense.AI:

CloudDefense.AI, headquartered in Palo Alto, is a cutting-edge Cloud-Native Application Protection Platform (CNAPP) that provides end-to-end security for cloud infrastructures and applications. CloudDefense.AI integrates advanced technology and expertise, making it the ultimate solution for mitigating security risks from development to deployment.

Their state-of-the-art platform offers a full spectrum of security solutions, ensuring organizations can confidently protect their cloud environments. Covering every layer of security, CloudDefense.AI provides SAST, DAST, SCA, IaC Scanning, Advanced API Security, Container Security, CSPM, CWPP, CIEM, Kubernetes Security, and AI-SPM. Moreover, their exclusive CloudShield.AI technology guarantees continuous policy enforcement and proactive threat mitigation.

CloudDefense.AI enhances security with AI-driven remediation, attack path analysis, and automated risk assessment to reduce vulnerability noise and detect zero-day threats in real-time. This innovative approach boosts security efficiency, providing up to five times the value of traditional tools and establishing them as leaders in cloud security.

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

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