# CloudDefense.AI CEO Anshu Bansal on Zero Trust's Role in Modern Infrastructure Protection with Forbes

PALO ALTO, CALIFORNIA, UNITED STATES, July 4, 2024 / EINPresswire.com/ -- CloudDefense.AI CEO, Anshu Bansal, has recently shared critical insights on the importance of Zero Trust in protecting modern critical infrastructure in a recent Forbes article. In a world where data breaches and cyberattacks have become daily news, Anshu highlights the urgency of adopting a Zero Trust security model to address the vulnerabilities of today's cloud-powered, borderless infrastructure.
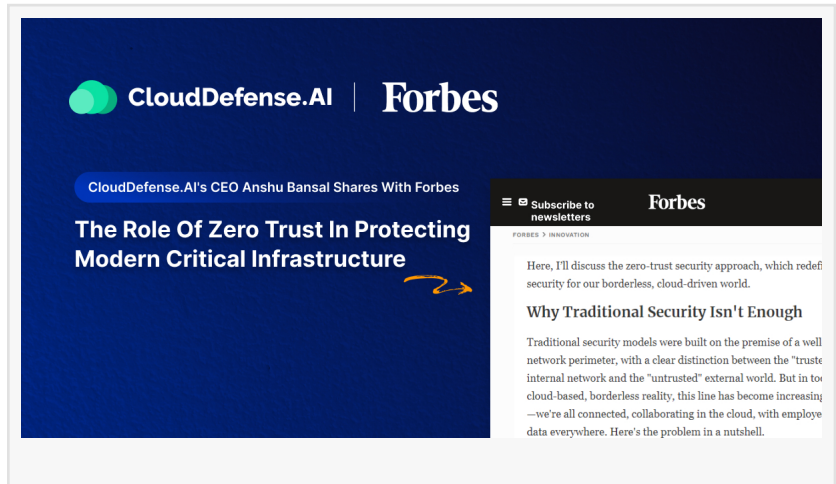
Anshu's article underscores the inadequacies of traditional security models that operate on the "trust but verify" principle, which is no longer sufficient in a landscape where the network perimeter is virtually non-existent. He points out that the rise of cloud adoption, remote work, BYOD policies, and the proliferation of connected devices have all contributed to the dissolution of clear network boundaries, creating a fertile ground for cyber threats. Hackers are exploiting these weaknesses by gaining unauthorized access, leading to significant data breaches.

> "
> Zero Trust is not just a modern security strategy; it is a necessary evolution to protect our critical infrastructure in today's interconnected world."
>
> *Abhi Arora, COO of CloudDefense.AI*

The Zero Trust approach, as Anshu explains, is a paradigm shift that fundamentally redefines security. It operates on the principle of "never trust, always verify," ensuring that every individual and device attempting to access network resources is continuously authenticated and authorized. This model enforces strict access controls, granting users the minimum necessary access to perform their tasks, thus minimizing potential damage from compromised accounts.

In his practical guide to implementing Zero Trust, Anshu emphasizes the importance of understanding one's attack surface through a comprehensive security risk assessment. This involves identifying critical assets and understanding the threat landscape to prioritize defenses effectively. He advocates for a strong Identity and Access Management system, micro-segmentation to isolate network zones, and Data Loss Prevention solutions to prevent sensitive data exfiltration.

Anshu also highlights the necessity of investing in the right security tools and expertise to support the Zero Trust model. Continuous monitoring and strong authentication mechanisms are essential to maintaining a strong security posture.

Read the full article [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.

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/725220025