Onclave Networks Emphasizes Growing Need to Protect Cloud-Based Infrastructure

Rise in cyberattacks creates an imperative to better protect data, devices, and workloads.

ONCLAVE

MCLEAN, VIRGINIA, UNITED STATES, October 20, 2022 /EINPresswire.com/ -- In response to industry research that shows organizations are facing an increasing number of cloud security breaches, Onclave Networks, a leader in Zero Trust security for IoT and connected devices, has released a white paper that examines the vulnerabilities of the cloud and solutions for protecting cloud assets.

As organizations shift to cloud environments to address industry-specific functionality, compliance needs, and supporting enterprise workloads, cyberattacks are also expanding to the cloud. In a recent IDC-commissioned cloud security survey, 98% of businesses reported they had experienced a cloud security breach within the last 18 months – up from 79% the previous year.

In the whitepaper, “Protecting Our Growing Cloud-based Infrastructure,” Onclave Networks covers the importance of increased employee responsibility, identifying misconfiguration, deploying Zero Trust Architecture (ZTA), and using solutions that provide containment and encryption of workloads from connected devices as essential to combating cyberattacks at the enterprise level.

There are over 85% of enterprise workloads currently in the cloud, more than 95% of all enterprises using cloud services, and over 40% of small and mid-sized businesses prefer a public cloud over on-premise storage. The private sector has embraced cloud services. On average, modern organizations are leveraging five different cloud platforms for day-to-day operations.

In addition to the rise in the adoption of cloud computing, every institution leveraging cloud services in 2022 has grown increasingly susceptible to security breaches and cyberattacks. IDC reported that 67% of corporate CISOs had experienced three or more security-related incidents since March 2021. IDC estimates that by 2025, there will be more than 55.7 billion connected devices, and 75% will feature IoT connectivity which is estimated to produce 73 zettabytes of data. Every one of them opens a door to the enterprise.

With the surge in digital transformation, innovation, and migration to cloud-storage implementation, the number of attacks will continue to rise. Additionally, the way we work, connect, and, most crucially, access information will all be revolutionized by 5G and IoT. When company data is exposed as a result, traditional IT security approaches prioritizing perimeter protection will not be effective.

“Organizations are recognizing that cloud providers are not able to ensure security for IoT and connected devices on the network,” said Don Stroberg, CEO of Onclave Networks. “This significant security vulnerability requires a specialized approach and a cybersecurity strategy that is agile, efficient, and risk-based. Having a solution specifically designed to work with your new or existing infrastructure is critical to identify and protect these vulnerable devices from a data breach.”

The requirement to defend the far end of the tunnel to the cloud locations will become vital to future-proof workloads moving from edge to cloud. It will be significantly more important to have a Zero Trust-based platform that is equipped with cryptographic microsegmentation capabilities to protect cloud-based infrastructures.

The Onclave TrustedPlatform™ is a Zero Trust network overlay that protects networks by cryptographically securing vulnerable OT and IoT workloads. By wrapping each workload in its own root of trust, the TrustedPlatform helps to eliminate the OT/IoT attack surface and ensure each segment is secure, whether it remains on-premises or travels across private, public, or hybrid cloud environments.

For more information on how to protect vulnerable workloads, devices, and systems connected to the cloud from increasing cyberattacks, read our whitepaper, “Protecting Our Growing Cloud-based Infrastructure”.

About Onclave Networks, Inc.

Onclave Networks, Inc. (McLean, Virginia) is a global cybersecurity leader securing new and legacy Internet of Things (IoT), Operational Technology (OT) and other connected devices, including those using 5G. Onclave dramatically reduces cyberattack surfaces, breaches, network complexity, and costly overhead created by shared infrastructure — enabling a more efficient and secure way to operate and communicate. Delivering an integrated solution based on Zero

Trust microsegmentation and leveraging proven methodologies used by the U.S. Department of Defense (DoD), Onclave is well-positioned to protect vulnerable endpoints across all sectors, on-premises and in the cloud. Onclave brings real trust to communications by securing networks from edge to cloud. For more information, visit our website, contact us, or download our white papers.

Ellen Koh
Onclave Networks, Inc.
ekoh@onclavenetworks.com
Visit us on social media:
Twitter
LinkedIn
