Case Study

Zscaler Deploys Confidential Computing with Intel® Trust Authority to Scale Zero Trust Across the Cloud

At a Glance

With this implementation, Intel and Zscaler help provide Silicon-to-Cloud security that scales across multiple applications, multi-tenants, and multi-cloud deployments.

The Challenge

With the complexity of today's connected environment—including the sheer number of devices and users, public and private clouds, and as-a-Service offerings—the threat landscape is requiring companies to adopt a Zero Trust approach to security. Furthermore, fast, secure access to cloud resources is critical to IT.

Cloud service providers are seeking solutions that build on security rooted in the hardware and that can easily scale across multiple clouds to verify the trustworthiness of the compute environments in which their applications run.

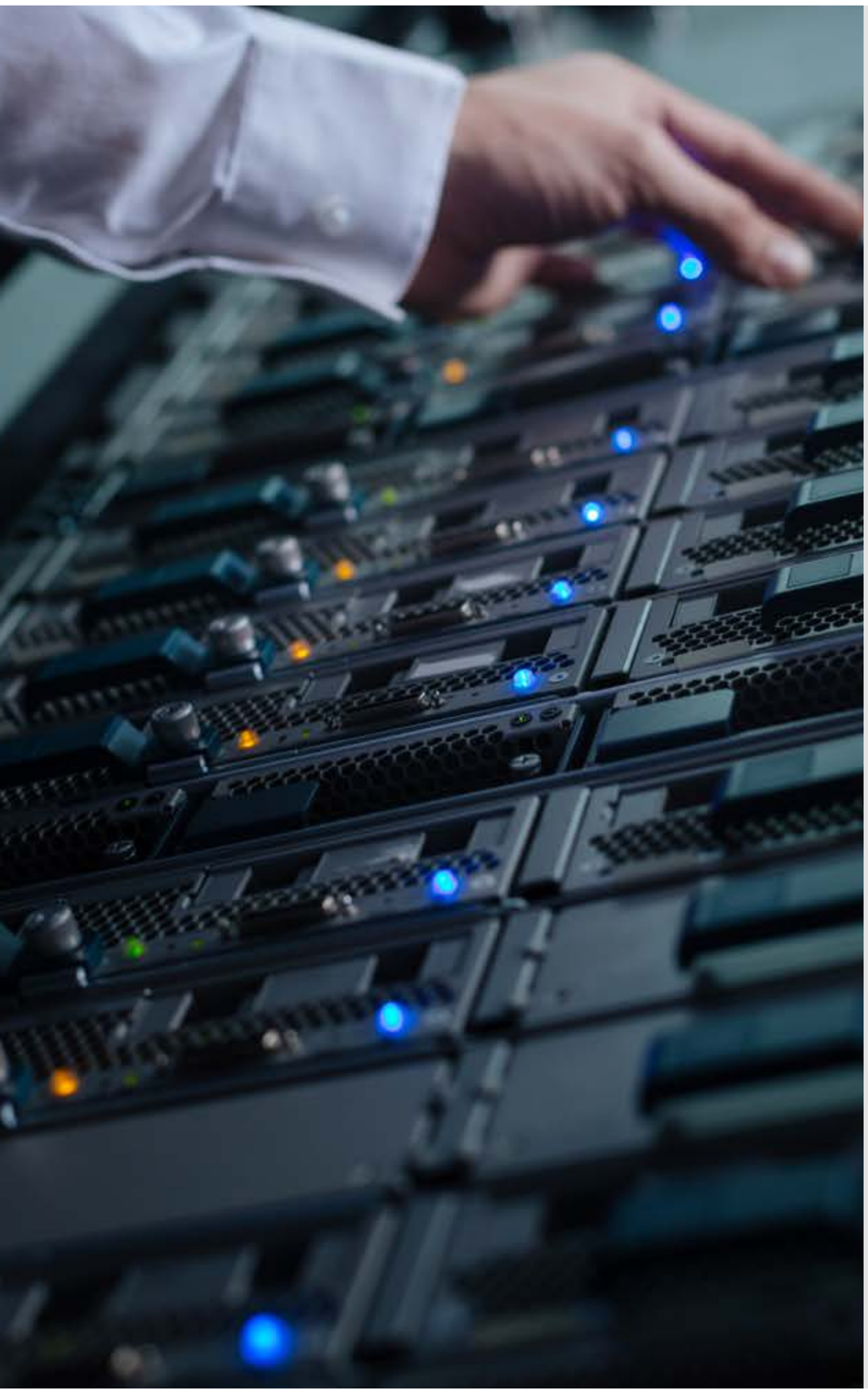
The Solution

Zscaler's cloud native Zero Trust Exchange platform securely connects users, devices, and applications in any location. In partnership with Intel, Zscaler is further enhancing security and scaling zero trust across multiple clouds by isolating its Zero Trust Exchange and App Connectors in silicon-based Intel® Trust Domain Extensions confidential computing environments and using Intel® Trust Authority to verify their authenticity and integrity (across multiple cloud infrastructures).

- Anchor trust in the silicon and scale it across multiple cloud environments.
- Cloud-native platforms and cloud-based applications mutually attest before running workloads.

"Zero Trust gives organizations the ability to operate more securely in IT environments where they can't verify directly that users, devices, or network infrastructure are secure and who/what they claim they are. Intel® Trust Authority takes that security one step further and verifies the computation path from apps to silicon can be trusted. With Confidential Computing and attestation services powered by Intel, we are entering the era of Zero Trust Silicon to Cloud."

– Ken Urquhart
Global Vice President of 5G Strategy



Fast. Secure. Verified.

Zscaler's cloud-native platform Zero Trust Exchange connects with multiple Zscaler App Connectors, which reside all over the world to facilitate fast and secure connections with customer applications. The App Connectors provide a secure authenticated interface between a customer's servers and the Zscaler cloud. In the pilot, Zscaler isolated and protected both Zero Trust Exchange and the many App Connectors in Intel TDX-based confidential computing environments, and then verified those environments using the SaaS-based Intel® Trust Authority.

Mutual Attestation of Cloud-Native Applications:

Before Zscaler connects an authenticated user to their requested workload, Intel® Trust Authority generates an attestation token for the Zero Trust Exchange to the App Connector, and for the App Connector to the Zero Trust Exchange, verifying that neither application has been tampered with. The workload can then be decrypted and executed inside the Intel TDX-based confidential computing environment.

intel

Printed in USA 0920/CCZ/TAN/PDF Please Recycle 356911-001US