CUSTOMER SUCCESS STORY

Zentera Readies Ambarella for 100% Work From Home, in Days

Work From Home

Remote Terminal

Data Leak Prevention

As the world adjusted to the post-pandemic paradigm, Ambarella needed a solution to allow its worldwide employees and contractors to switch to fully-remote working without sacrificing security in the process. Zentera worked with Ambarella to implement Zero Trust Network Access and helped the company onboard its global workforce in just one week.

The Challenge

Ambarella is one of the world's most innovative semiconductor companies, creating silicon to power AI and computer vision applications for autonomous driving, among other applications. Naturally, development of these advanced applications generate significant Intellectual Property (IP). Many of the Ambarella staff were used to engaging with company IP onsite; processes, procedures, operations, and safeguards around interacting with this IP were well-developed and robust. Then, COVID-19 happened.

Ambarella™

Ambarella's products are used in a wide variety of human and computer vision applications, including video security, advanced driver assistance (ADAS), electronic mirror, drive recorder, driver/cabin monitoring, autonomous driving, and other robotic applications. Ambarella's low-power and high-resolution video compression, image processing, and deep neural network processors and software enable cameras to become more intelligent by extracting valuable data from high-resolution video streams.

INDUSTRY

Semiconductors - AI

HEADQUARTERS

Santa Clara, CA

ZENTERA PRODUCTS

CoIP® Access Platform
Zentera Secure Access

zentera™

Customer Success Story

Zentera Readies Ambarella for 100% Work From Home, in Days

As Ambarella employees around the globe started working from home, the IT team had to make a choice: either give everyone VPN access, extending the corporate infrastructure to remote for expediency, or find a better and more secure solution.

The existing corporate VPN was originally deployed to connect company-owned, trusted and managed laptops back to the corporate network. However, not every employee had such a company laptop. Given the fact that the Wi-Fi and other devices in the home environment may not be trusted, extending VPN access to these personal laptops would create new scenarios to evaluate for risk and compliance.

Additionally, while VPN access to less critical assets was an established procedure, the more sensitive IP was kept in more secure zones in the internal network. Opening the network for this access would potentially weaken internal security controls and expose corporate assets to higher risk. Of course, business continuity is paramount – unless they could find a better way.

New Technology Preserves Existing Workflows

Rather than define a completely new solution and introduce new and unknown security risks, Ambarella worked with Zentera solution architects to define a solution to leverage the best of the existing infrastructure while protecting their critical IP.

Ambarella adopted Zentera Secure Access (ZSA), using it to provide its employees and contractors with secure remote terminal access terminating directly to the user's corresponding desktop machine in the secure zone on-premises. Based on the CoIP Access Platform and following the principles of Zero Trust, ZSA allowed Ambarella to lock the access to whitelisted RDP and VNC binaries. Authenticated users on BYOD machines could view and manipulate data, while copy/paste and file transfer capabilities were blocked to safeguard the critical IP, as were other applications on the BYOD machine.

Key Objectives

- Support instant Work From Home access to critical intellectual property
- Secure IP when accessed from untrusted laptops and networks
- Leverage existing compliance frameworks and security models without changing any existing infrastructure, for rapid deployment

The Solution

- Zentera Secure Access for secure remote terminal access overlay on existing infrastructure
- Secure RDP/VNC with copy/paste and file transfer functions disabled
- VPN-less connection locked for the purpose
- User authentication backed by existing corporate directory

Business Benefits

- Ensured business continuity
- Improved Data Leak Prevention security when connecting remote users
- No impact to existing security, compliance, and network infrastructure

Zentera Readies Ambarella for 100% Work From Home, in Days

Going From Zero to 100 in 7 Days

With ZSA, user onboarding was simple. Ambarella IT installed the zLink agent to each of the on-premises desktops, and then connected the service to their corporate identity provider to authenticate user logins.

They then imported policies mapping users to target desktops into the zCenter orchestrator. This associated users to their desktops, with IdP-backed authentication.

Users received onboarding instructions, and once logged in, were immediately presented with their desktop resource and no others.

In just days, Ambarella was able to deploy and configure service, and onboard over 700 worldwide users in multiple regions, with access methods that support their existing, compliant workflows, and provide peace of mind and security for access from untrusted BYOD devices and networks.

ZSA allowed Ambarella to ensure business continuity without having to purchase and provision new corporate laptops, re-engineer corporate network infrastructure, or reconfigure internal security controls. ZSA also saved the company significant time and money compared to alternate solutions such as VPN and virtual desktop infrastructure, which would have required new builds and intensive security evaluations.

Supporting a Worldwide Workforce

As a global organization, Ambarella maintains operations on three continents. The company decided to deploy ZSA in each of its major regions to optimize performance and minimize latency for its users.

Zentera's appliance-based models made it simple for Ambarella's local IT teams to quickly deploy on-premises in each region, without having to evaluate and navigate complex service contracts and options.

> " Zentera Secure Access has been a critical enabler for our Work From Home program, providing increased security and avoiding re-engineering that could have impacted our compliance and productivity. Our users get a simple flow that they know and understand, and don't need retraining. "
>
> Sr. Director of IT
> Ambarella, Inc.