CASE STUDY

Adobe Finds ZEN Using Identity-Centric Security

Overview

As with most organizations that are facing digital transformation initiatives, Adobe faced the challenge of finding the right balance between a pleasant user experience and stringent security requirements. With the increasing complexity of user authentication being driven by enhanced security policies, for example blending usernames and passwords with second factor authentication, the user experience began to suffer. In many cases users needed to re-authenticate many times a day depending on the applications or devices they use. Den Jones, Director of Enterprise Security, took on this challenge and is achieving the perfect balance through a Zero-trust Enterprise Network (ZEN) approach.

As the Adobe team began evaluating their current state, they ran across a number of hurdles that needed to be addressed. Internal application access was outdated and did not adhere to cloud-like concepts that are more prevalent today. Their application authentication and authorization standards were not consistent and not being enforced. Single Sign-on was not being deployed across applications. In addition, device security was not being enforced, including access to restricted data. Any device could join the network with network level access to almost all of the data center infrastructure. The Adobe team was asked to address these issues, while leveraging existing technology investments such as authentication, network access control, logging, endpoint detection and response and device management

Solution

The Zero-Trust Enterprise Network (or ZEN) project from Adobe is an initiative based upon numerous best practices and principles from various digital workspaces, including the Identity Defined Security Alliance. The ZEN architecture allows Adobe to achieve the goal of tighter security and a positive user experience. Adobe was able to offer a VPN-free method of seamlessly accessing applications and replaced usernames and passwords with certificate-based authentication. For any application accessible through the ZEN platform, Adobe evaluates the security posture of each device attempting access. Therefore, a user will only be required to authenticate, as needed and based on security policies.

In addition to delighting users, ZEN helps reduce the risk of unwanted lateral movement within the network during an incident or breach scenario.

Industry
- Technology

Challenge
- Transform network and applications to a "cloud-like" state
- Enable application access without the need to be internal or use VPN
- Secure network level access based on user and device posture

Solution
- Deploy a zero trust approach to security using identity-centric principles
- Leverage existing identity and security technology investments

Lessons Learned
- Identity-centric security approach is needed, but an off the shelf solution does not exists
- Bringing together vendors to meet the requirements is time consuming
- IDSA provides practical guidance and forum for peer to peer support

IDSA Use Case
- Access Management Verifies Enterprise Mobility Management Status of Mobile Device

IDSA Member Technologies
- Okta
- VMware Workspace ONE

"Working with the IDSA is a great opportunity to help drive innovation across the tech industry with vendors and solution providers alike. Adobe benefits through exposure to vendors, use cases and community best practices that help elevate and strengthen our identity and security teams." **Den Jones, Director of Enterprise Security, Adobe**