As applications, users, and devices evolve, dissolving what was once the trusted enterprise perimeter, many businesses are turning to a zero trust security model to secure against attacks. Use this step-by-step guide from Akamai’s CTO, Charlie Gero, to build an inclusive and concrete zero trust architecture, intended to help enable safe application access in a rapidly evolving world. Early transition to a perimeter-less environment with this prescriptive process, phasing applications in at a time and reducing your migration risk profile.

1. Application Precheck Stage
   First, check to make sure the application meets the requirements of the access proxy you have deployed. Find more about pre-staging assumptions and necessary prerequisites in this white paper, authored by Charlie Gero.

2. Access Proxy Preparation Stage
   Next, configure your access proxy to support the application as well as its specific security and access rights. Consider the environment in which this will be configured — cloud versus on-premises — and how it will be pushed to your end users.

3. Test Lab Enrollment Stage
   Now you can begin enrolling users. We recommend a designated Test Lab group be previously established, these users will be those first responsible for analyzing the functional integrity of the application. By this time, Test Lab members should confirm that authentication is working correctly, multi-factor authentication is appropriately configured, and single sign-on works across all other previously onboarded applications. For more information about user grouping methodology, read the white paper.

4. Security Upgrade Stage
   Once Test Lab users are safely able to access the application, you should begin analyzing advanced security features were necessary in the traditional perimeter model. We recommend:
   - Web application firewall (WAF) for SQL injection, cross-site scripting, and cookie injection attacks
   - Advanced threat protection
   - Browser and operating system governance
   - Restrictions for unmanaged versus managed devices
   - Geocoding and IP-based limitations
   Regardless of the features you enable, Test Lab members should ensure that the security options are not only working, but also are not inhibiting the functional correctness of the application.

5. Performance Upgrade Stage
   You should now examine performance degradation. In traditional access and security models, enterprises are often limited in performance by the robustness of the application server and the enterprise’s associated links between branch locations. Features we recommend to mitigate these issues include:
   - Caching
   - Utilizing a content delivery network (CDN)
   - Server optimization
   - Protocol optimization
   - Geoblocking and IP-based limitations
   - Restrictions for unmanaged versus managed devices
   - Browser and operating system governance
   - Advanced threat protection
   - Web application firewall (WAF) for SQL injection, cross-site scripting, and cookie injection attacks

6. External User Enrollment Stage
   At this point, all users are external users, and as such, access necessitates VPN removal for the group. External users are also most often affected by performance issues and are in the most hostile environments — their very location puts your applications and data at risk. While the transition should be nearly invisible, available from increased performance, we recommend advanced notification to users so that they can keep a close eye on functional correctness. For more information about user grouping methodology, read the white paper.

7. Internal User Enrollment Stage
   At this point, your users will apply the application as a CNAME (Canonical Name) entry to the common view. All users should then immediately begin accessing this application via the access proxy. Hopefully, through the prior six stages, any errors or misconfigurations will have been discovered and remedied; all users should now be enjoying the benefits of easier, faster, and safer access. For more information about user grouping methodology, see the white paper.

8. VLAN Migration Stage
   After an appropriate amount of time has passed, you can shift the application into the walled-off VLAN before the access proxy is disabled. Remember to remove all access until you are sure the application is working correctly, multi-factor authentication is appropriately configured, and single sign-on works across all other previously onboarded applications. For more information about user grouping methodology, read the white paper.

Review Akamai’s zero trust reference architecture to visualize this prescriptive process or visit akamai.com/zerotrust to learn more about the solutions that can assist you with the above implementation.