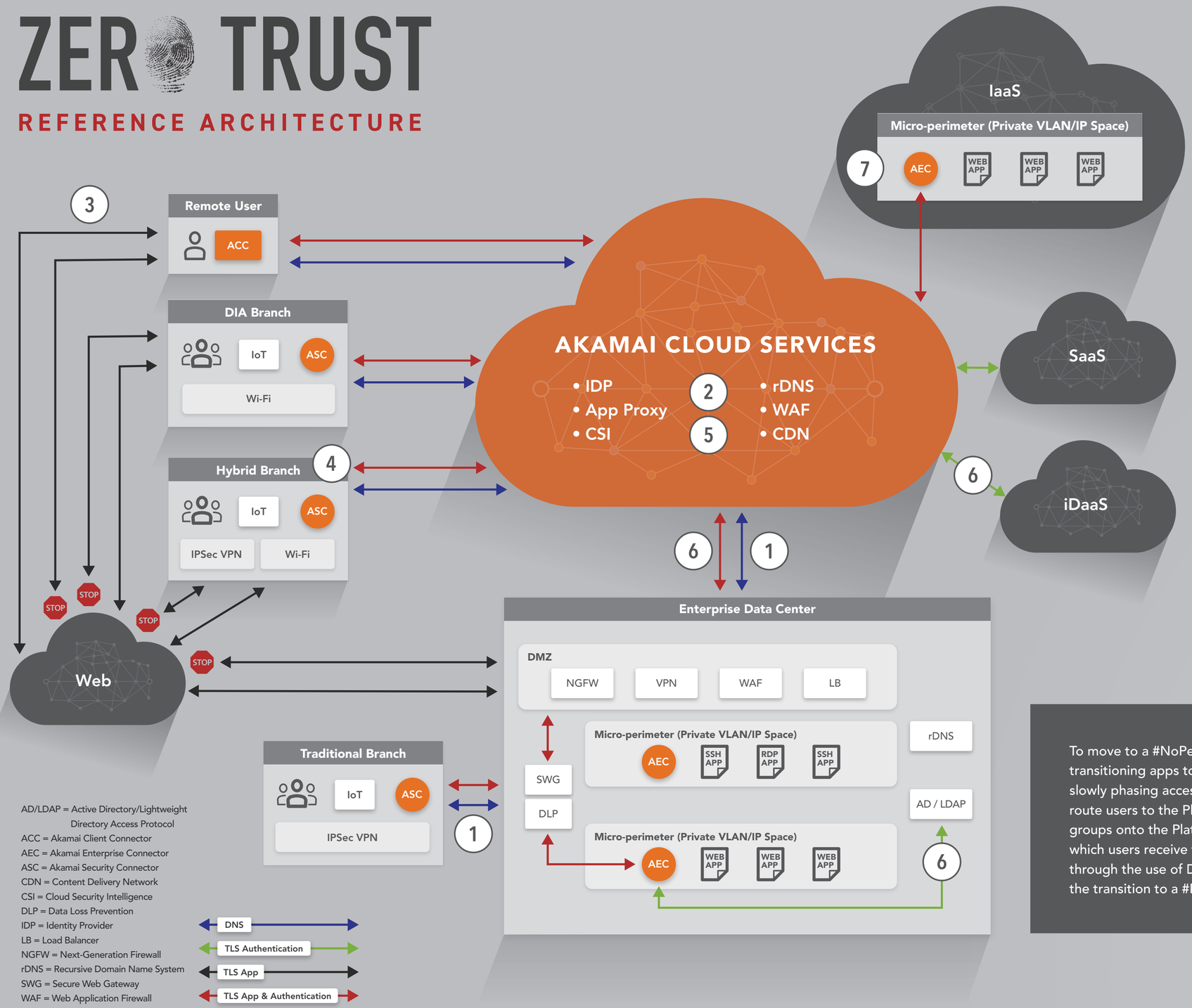
ZERO TRUST

REFERENCE ARCHITECTURE



1. The user makes a DNS request for an enterprise app or domain on the web. The local enterprise rDNS infrastructure, or the Akamai Client Connector (ACC) if off-network, forwards the request to the Akamai rDNS Platform.

2. Akamai evaluates the domain against Akamai's Cloud Security Intelligence (CSI) to determine whether it is known or suspected to be malicious.

3. If the domain is not malicious, Akamai's infrastructure will hand back the appropriate IP to the destination on the web or the Akamai Platform for enterprise app access authentication and authorization.

4. If the domain is malicious, or inappropriate based on configured policy, the Akamai Platform will either block access or hand back the internal IP of the Akamai Security Connector (ASC). The ASC will capture the internal IP of the endpoint making the malicious request and send that over TLS to Akamai CSI for correlation to facilitate endpoint identification.

5. If the domain was for an enterprise app on the Akamai Platform, it will use the CNAME process to hand out the appropriate IP to the WAF, CDN, IDP, and App Proxy functionality on the Akamai Platform.

6. The Akamai Platform will serve a login page, optionally using a client certificate for initial authentication, and use the Akamai Enterprise Connector (AEC) to validate that the user and password exists in the appropriate identity store (IDaaS, Akamai IDP, and AD/LDAP on-prem) to authenticate the user, (optionally triggering Multi-Factor Authentication) and authorize specific app access.

7. The AEC will leverage a mutually authenticated TLS connection (outbound only) with the Akamai Platform, and the TLS connection from the user's browser, to create a proxied path across the Akamai Platform from the end user to the application. For configured SaaS apps, Akamai will handle authentication and authorization only, but for other apps, will log access details.

To move to a #NoPerimeter security model that embraces zero trust and BeyondCorp™ ideologies, begin transitioning apps to the Akamai Platform in small batches. Part of the application transition will involve slowly phasing access to select user groups. Application hostnames are CNAME'd to Akamai in order to route users to the Platform. Take advantage of this architecture as a way to phase the different user groups onto the Platform for each application by controlling which groups follow the CNAME chain and which users receive the internal A-record using the outdated perimeter method. This can be achieved through the use of DNS Views, also known as split-horizon DNS, to define the set of users and facilitate the transition to a #NoPerimeter security model. To learn more, visit akamai.com/zerotrust.

carahsoft. Akamai