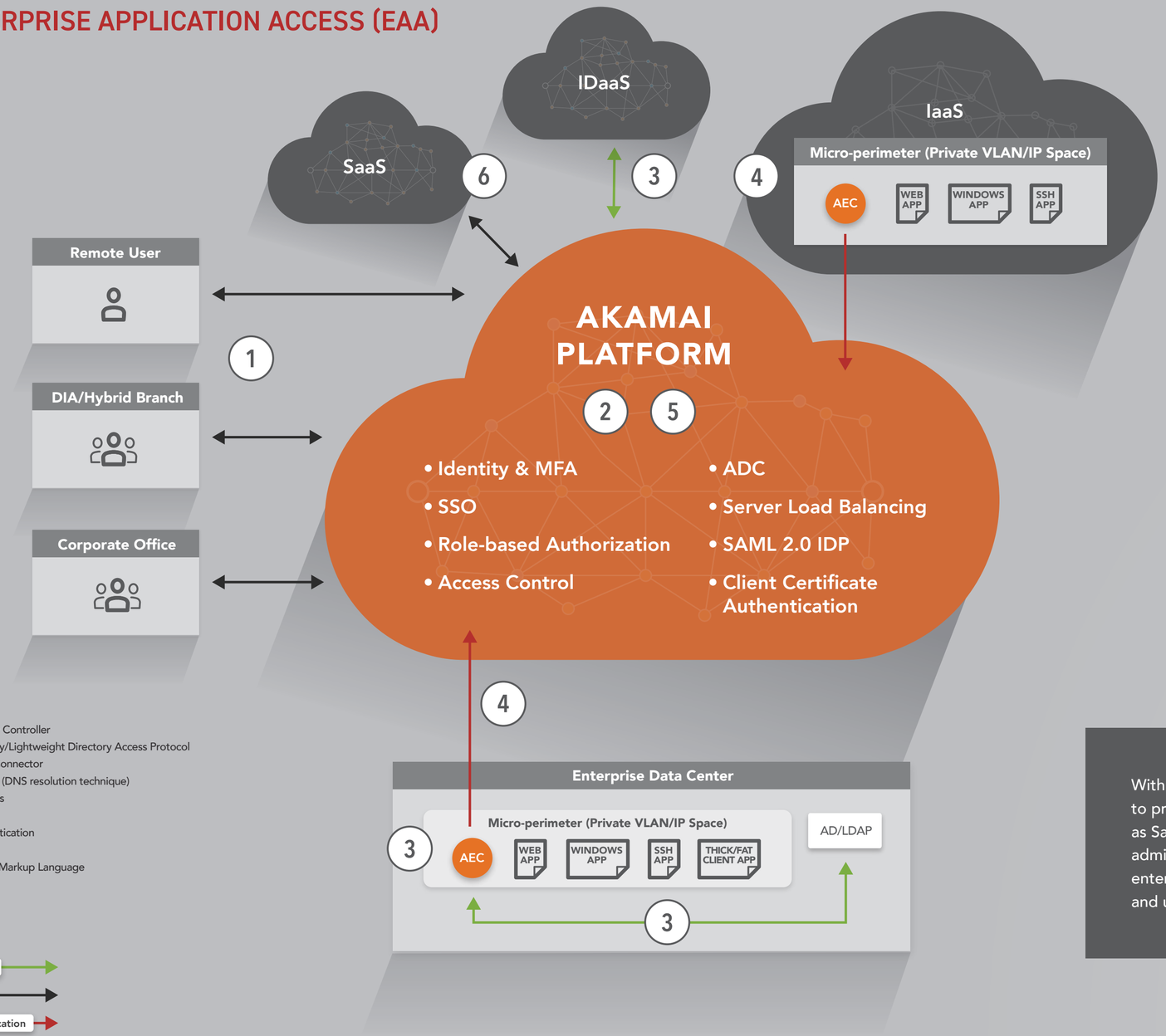
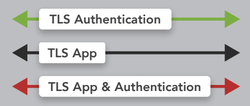
AKAMAI CLOUD SECURITY

SINGLE SIGN-ON ACROSS ALL APPLICATION TYPES WITH ENTERPRISE APPLICATION ACCESS (EAA)



ADC = Application Delivery Controller
AD/LDAP = Active Directory/Lightweight Directory Access Protocol
AEC = Akamai Enterprise Connector
CNAME = Canonical Name (DNS resolution technique)
DIA = Direct Internet Access
IDP = Identity Provider
MFA = Multi-Factor Authentication
NTLM = NT LAN Manager
SAML = Security Assertion Markup Language
SP = Service Provider
SSO = Single Sign-On



1. The user accesses an enterprise or SaaS app hostname published through Enterprise Application Access (EAA). Through CNAME redirection process, the request will come to Akamai EAA Edge.

2. The Akamai EAA Edge will serve a login form, optionally using a client certificate and/or MFA for initial authentication, and will validate that the user and password exist in the Akamai identity store (AD or OpenLDAP).

3. The EAA Edge sends the authentication request to the Akamai Enterprise Connector (AEC), which works as the LDAP client to validate the credentials in the appropriate identity store (AD/LDAP) for authentication and role-based authorization. In case the identity store is configured as IDaaS, EAA Edge redirects the user request to IDaaS using SAML 2.0 integration.

4. The EAA Edge will leverage mutually authenticated TLS connections (outbound only) from the AEC in order to create a proxied path across the Akamai Platform, from the end user to the application. The AEC can also be leveraged for ADC capabilities, application server load balancing, injecting HTTP headers, SSO authentication bridging via Kerberos/NTLM, etc.

5. After successful authentication, a secure cookie is set for the user session. Role-based authorization and other access control policies are also enforced before access is granted to any type of application. This is done via a unified application landing page that displays authorized application tiles. Optionally, users can access the applications directly using external hostnames.

6. In case of SaaS access, the user can access the app directly using an external hostname or through an application landing page. EAA Edge acts as a SAML 2.0 IDP to broker connectivity between the SAML SP (SaaS application) and the user. After presenting credentials to the login form and successful authentication/authorization, EAA Edge starts a SAML transaction with the SP (SaaS application) and the user gets an SSO experience.

With the inclusion of SAML 2.0 IDP, we round out Enterprise Application Access' IDP offering. EAA is able to provide seamless SSO beyond on-premise and IaaS, and can support any SAML 2.0-compliant app such as Salesforce, Microsoft Office 365, Workday, Dropbox, ServiceNow, or G Suite. Both end users and IT admins will be able to leverage Akamai EAA as their launchpad for SaaS applications, as well as their enterprise applications hosted in the data center or in the public cloud. EAA's IDP offers true seamless and unified sign-on to all internal applications.

Visit **akamai.com/eaa** to learn more.

Akamai