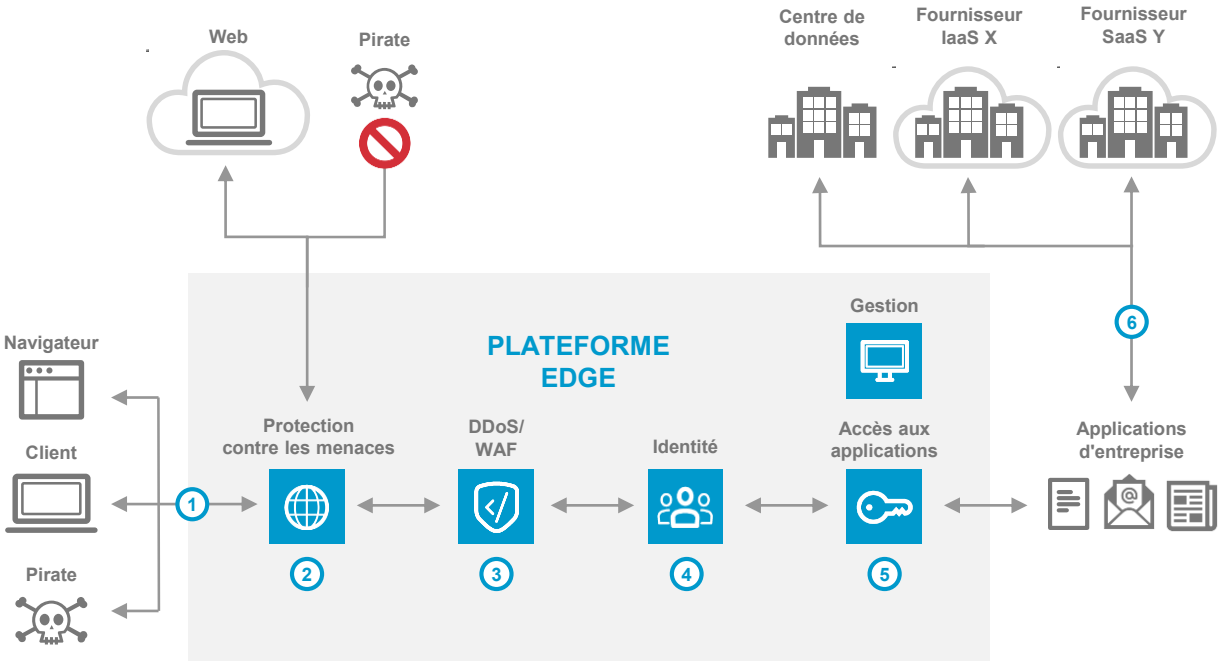
LA SÉCURITÉ ZERO TRUST

Architecture de référence



PRÉSENTATION

Une architecture de sécurité Zero Trust minimise le risque que des acteurs malveillants pénètrent dans le périmètre, se déplacent latéralement et exfiltrent des données. Grâce à des privilèges minimaux et une politique de refus par défaut, Zero Trust vous permet de protéger les utilisateurs et de leur fournir un accès via un ensemble unique de contrôles de sécurité et d'accès, tout en adaptant les ressources limitées aux besoins de l'entreprise.

1. Les utilisateurs accèdent aux applications d'entreprise et au Web via Akamai Intelligent Edge Platform.
2. La protection contre les menaces protège les utilisateurs contre les programmes et les contenus Web malveillants ainsi que l'hameçonnage, tout en offrant une visibilité à l'entreprise.
3. Concernant les applications d'entreprise, les serveurs en bordure de l'Internet bloquent automatiquement les attaques DDoS au niveau de la couche réseau et vérifient l'absence de menaces telles que les injections SQL, les attaques XSS et les inclusions de fichiers à distance (RFI).
4. L'identité de l'utilisateur est établie à l'aide de systèmes d'identification d'Akamai, sur site ou dans le cloud.
5. En fonction de son identité et d'autres signaux de sécurité, l'utilisateur peut accéder uniquement aux applications requises et non à l'ensemble du réseau de l'entreprise.
6. Akamai Intelligent Edge Platform achemine les utilisateurs autorisés et authentifiés vers les applications d'entreprise concernées.

PRODUITS CLÉS

Protection contre les menaces ► Enterprise Threat Protector
DDoS/WAF ► Kona Site Defender ou Web Application Protector
Accès aux identités et aux applications ► Enterprise Application Access

Akamai