SOLUTION BROCHURE

Assurer la conformité cloud et cybersécurité au Maroc

Loi 05-20 · Décret 2-24-921 · Arrêté 3-17-25 (B.O. n° 7432)

ENTRUST

SECURING A WORLD IN MOTION

Présentation générale

Chiffrez vos données sensibles dans le cloud tout en gardant la maîtrise des clés de chiffrement. Avec Entrust, la gestion des clés et les contrôles d'accès restent sous votre gouvernance, avec une traçabilité adaptée aux audits et aux exigences locales.

Contexte réglementaire

Le cadre marocain (Loi n° 05-20, Décret n° 2-24-921) impose des exigences de protection pour les systèmes et données sensibles hébergés dans le cloud. L'Arrêté n° 3-17-25 définit les critères de qualification des fournisseurs de services cloud. Les organisations doivent démontrer un chiffrement robuste, une gestion rigoureuse des clés, une séparation des rôles et une traçabilité complète. La mise en conformité est attendue d'ici fin 2026.

Note : ce document est fourni à titre informatif et ne constitue pas un avis juridique. L'interprétation et l'application des exigences peuvent varier selon le contexte et doivent être confirmées par vos équipes conformité/juridique.

Alignement réglementaire

Exigence réglementaire	Capacité Entrust
Contrôle exclusif des clés de chiffrement par le client	Entrust CSP Key Manager (ci-après « CSP Key Manager ») : administration des clés et politiques sous contrôle du client
Absence d'accès du fournisseur cloud ou du prestataire aux clés	HYOK (Hold Your Own Key) : le client détient les clés; accès limité, contrôlé et auditable
Gouvernance cryptographique renforcée	Cycle de vie des clés centralisé pour appliquer des politiques cohérentes
Protection contre les menaces internes	Entrust nShield HSM (option) : clés non exportables pour réduire l'exposition
Préparation aux audits et à la conformité	Journaux et rapports prêts pour l'audit (Entrust Compliance Manager)

Architectures possibles pour la maîtrise des clés et l'isolement

Les options ci-dessous couvrent différents niveaux d'isolement (accès, séparation opérationnelle, sauvegarde/restauration) afin de répondre aux exigences de maîtrise des clés et de traçabilité. Pour les modèles mutualisés, les limites doivent être documentées et partagées en amont.

Option 1 — Appliance CSP Key Manager partagée avec plusieurs Vaults (un Vault par client)

- Une appliance CSP Key Manager.
- Plusieurs Vaults KMIP (Key Management Interoperability Protocol), un par client.
- Sélection du Vault via des certificats dédiés.

Points forts

- Coût d'infrastructure réduit.
- Moins d'appliances à déployer et maintenir.
- Supporté par VMware (KMIP + mapping par certificats).
- IdP distinct possible par Vault, selon la gouvernance du client.

Limites / points d'attention

- Isolation limitée (appliance et stockage sous-jacent mutualisés).
- Sauvegarde/restauration non isolées par client.

Note : ce modèle présente des contraintes d'exploitation et de conformité qui doivent être clairement communiquées dans le dossier d'architecture (mutualisation et sauvegarde/restauration).

Option 2 — Appliance partagée + un Vault par client + ressources VMware dédiées (vSAN / vCenter par client)

- Une appliance CSP Key Manager partagée.
- Un Vault par client.
- Chaque Vault protège des ressources VMware dédiées (vSAN/vSphere séparés par client).

Points forts

- Séparation logique renforcée vs Option 1.
- Réduit le nombre d'appliances à opérer.
- Compatible avec les contraintes VMware (unit-of-protection).

Limites / points d'attention

- Appliance et stockage mutualisés (isolement partiel).
- Prérequis : ressources VMware réellement dédiées par client.
- Sauvegarde/restauration : isolement encore limité.

Note : cette option suppose une séparation effective de l'infrastructure VMware par client (par exemple vSAN/vSphere dédiés). Ce prérequis doit être validé en amont.

Option 3 — Une appliance CSP Key Manager par client (un Vault par appliance)

- Une appliance CSP Key Manager par client.
- Un Vault par appliance.

Points forts

- Isolement maximal (clés, Vaults, opérations, sauvegardes).
- Simplifie la conformité et les audits.
- Réduit les risques et les cas limites liées à la mutualisation.

Limites / points d'attention

- Coût plus élevé.
- Exploitation à l'échelle : supervision, mises à jour, capacité.

Note : un déploiement « une appliance par client » simplifie l'exploitation, clarifie le périmètre d'audit et réduit les ambiguïtés liées à la mutualisation.

Recommandation (générique)

Lorsque l'exigence est une isolation forte (maîtrise des clés, séparation opérationnelle et audit), privilégier une appliance par client (Option 3). Les Options 1 et 2 restent possibles si la mutualisation est acceptée, avec limites et prérequis clairement formalisés.

Synthèse

Accélérez votre adoption du cloud au Maroc avec un chiffrement à contrôle client, conçu pour faciliter la conformité et la préparation aux audits. Entrust vous aide à démontrer la maîtrise des clés, la séparation des rôles et la traçabilité, avec un modèle de déploiement ajustable à votre niveau d'isolement attendu.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION