

EVERTRUST POUR LA GESTION DE LA POSTURE CRYPTOGRAPHIQUE

MAÎTRISEZ VOTRE CRYPTOGRAPHIE. REMÉDIEZ AUX VULNÉRABILITÉS.

PROUVEZ VOTRE CONFORMITÉ.

Pilotez votre posture cryptographique et démontrez votre conformité à tout moment. Evertrust CPM offre une vision exhaustive de votre patrimoine cryptographique et des risques associés, orchestre la remédiation de bout en bout et produit les preuves attendues par vos auditeurs.

L'ENJEU

Clés, certificats, algorithmes, bibliothèques : les actifs cryptographiques sont disséminés dans l'ensemble du SI, et leurs dépendances demeurent largement méconnues. **Faute de visibilité** sur les applications et services qui en dépendent, les organisations **peinent à évaluer leur exposition réelle et à prioriser la remédiation.**

La maîtrise de la posture cryptographique est pourtant **devenue une exigence réglementaire**, portée par DORA, NIS2, PCI DSS et eIDAS, et appuyée par les recommandations de l'ANSSI et du NIST. Elle constitue également le prérequis de toute **transition post-quantique** : **on ne migre pas ce que l'on ne connaît pas.**

L'APPROCHE EVERTRUST CPM

Evertrust CPM s'intègre à votre écosystème existant pour constituer un inventaire exhaustif de vos actifs cryptographiques et en cartographier les dépendances.

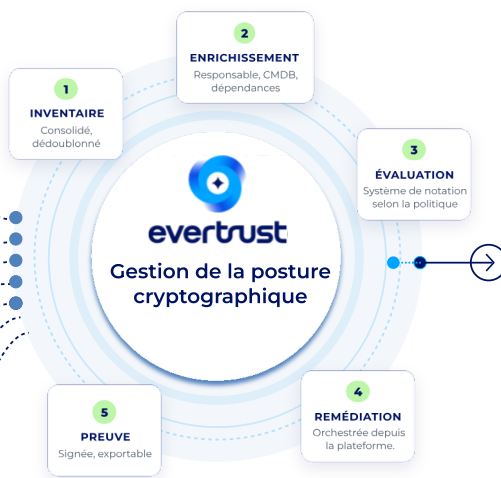
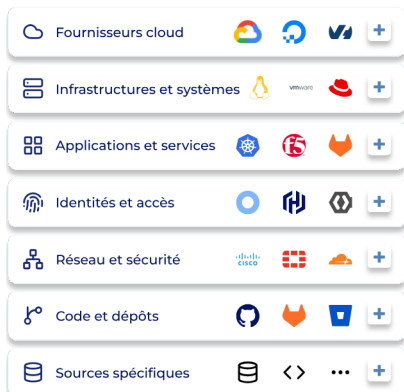
Chaque actif est évalué au regard de votre politique de sécurité, attribué à un responsable et priorisé en fonction de son impact métier. Vos équipes concentrent leurs efforts sur les risques majeurs, orchestrent la remédiation depuis leurs outils et disposent des éléments de preuve attendus par les régulateurs, ainsi que d'un socle fiable pour conduire la migration post-quantique.

FONCTIONNEMENT

UN CYCLE DE CONFIANCE : CARTOGRAPHIER, REMÉDIER, PROUVER

DÉCOUVERTE MULTI-ENVIRONNEMENTS

L'ensemble de vos actifs cryptographiques, **partout.**



INDICATEURS DE PILOTAGE

De la découverte à une posture cryptographique **maîtrisée.**



DÉPLOIEMENT AU CHOIX



On-premise
Au sein de votre périmètre.



SaaS
Opéré par Evertrust.

FONCTIONNALITÉS

UNE PLATEFORME. UN INVENTAIRE. UNE TRAÇABILITÉ DE BOUT EN BOUT.

1

Gouvernance par périmètre

Contrôle d'accès par rôles (RBAC) et cloisonnement par périmètre : chaque équipe ne voit et n'agit que sur les actifs dont elle a la charge, avec des habilitations définies action par action.

2

Couverture complète du SI

Serveurs, postes de travail, clusters, dépôts de code, coffres-forts, HSM, KMS cloud, équipements réseau et scanners de vulnérabilités. Toute autre source se raccorde via des connecteurs personnalisés.

3

Contexte métier intégré

Chaque actif découvert est croisé avec votre contexte métier et rattaché à un responsable, un niveau de criticité et vos propres étiquettes. Chaque alerte parvient au bon interlocuteur, prête à être traitée.

4

Cartographie des dépendances

Chaque clé et chaque certificat est relié aux serveurs, services et applications qui l'utilisent, dans une cartographie actualisée à chaque découverte. Vous mesurez l'impact d'un changement avant de l'engager.

5

Conformité aux référentiels

Chaque actif est évalué au regard des référentiels du marché, ou de votre politique interne : algorithmes, longueurs de clés, durées de validité et protocoles. Chaque écart est détecté et noté.

6

Remédiation maîtrisée

Les actions de remédiation sont orchestrées jusqu'à l'exécution. Vos équipes agissent à grande échelle, sans risque pour la production et avec une traçabilité complète.

7

Migration PQC pilotée

Définissez votre trajectoire de migration par phases et jalons, directement dans la plateforme. L'avancement est mesuré sur les actifs réellement observés, et non sur du déclaratif.

8

Preuves d'audit à la demande

Des rapports adaptés aux auditeurs, à la direction et aux équipes conformité, évalués selon votre politique, versionnés et exportables en PDF, CSV ou via API.

CAS D'USAGE

DE L'INVENTAIRE À LA CRYPTO-AGILITÉ



GAGNER EN VISIBILITÉ

Un inventaire fiable, dès le premier audit

Constituez un référentiel exhaustif des actifs cryptographiques, de leurs responsables et de leurs dépendances, base de votre conformité comme de votre migration post-quantique.

Identifier l'exposition au risque quantique

Repérez les algorithmes vulnérables à l'informatique quantique et les systèmes critiques qui en dépendent, afin de savoir où commencer.



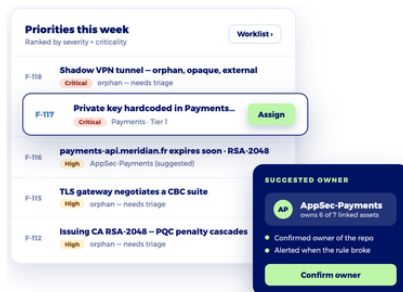
RÉDUIRE VOTRE EXPOSITION

Réagir à une dépréciation ou un retrait de confiance

Lorsqu'une autorité de certification ou un algorithme est déclaré non fiable, identifiez aussitôt les systèmes concernés et remplacez-les par ordre de criticité métier.

Éliminer la cryptographie non conforme

Détectez les écarts à votre politique (clés trop courtes, algorithmes faibles, protocoles dépassés) et corrigez-les à grande échelle par campagnes de remédiation.



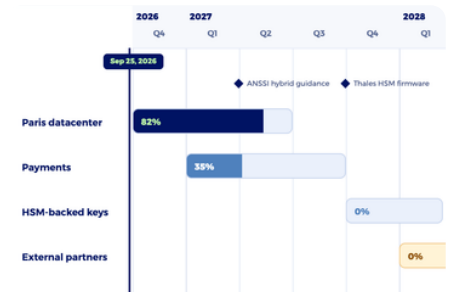
ANTICIPER LE CHANGEMENT

Gouverner la cryptographie à l'échelle du groupe

Appliquez une politique commune à l'ensemble de vos entités tout en déléguant la remédiation à chaque équipe sur son propre périmètre.

Piloter la migration post-quantique

Planifiez la migration par phases et jalons, et mesurez son avancement sur les actifs réellement observés, pour en rendre compte à la direction comme aux régulateurs.



À propos d'Evertrust

Éditeur français de solutions de confiance numérique, Evertrust donne aux organisations, en Europe et au-delà, la maîtrise de leur posture cryptographique : PKI, gestion du cycle de vie des certificats, inventaire cryptographique, crypto-agilité et préparation au post-quantique.

Abordez votre prochain audit de posture cryptographique en toute confiance.

contact@evertrust.io

Échanger avec un Expert