Hardened Docker Desktop

Sécurisez les postes de travail des développeurs à grande échelle

Sécurisez les postes de travail des développeurs à grande échelle

Chaque jour, les cyber-risques augmentent. Les dommages causés par les cyberattaques devraient atteindre 10 500 milliards de dollars d'ici à 2025. Ces risques - logiciels malveillants, attaques de la chaîne d'approvisionnement, mauvaises configurations, menaces internes, etc. - nous rappellent que la sécurité est nécessaire à chaque étape du cycle de développement des logiciels, depuis les premières étapes du développement (ordinateurs portables et bureaux virtuels des développeurs) jusqu'aux environnements de tests et de production.

Hardened Docker Desktop (HDD) fournit un ensemble de fonctionnalités de niveau professionnel qui sécurisent les postes de travail des développeurs sans les arrêter ni les ralentir, pour qu'ils puissent se concentrer sur ce qu'ils aiment le plus : écrire du code. Cette solution :

- Permet aux administrateurs informatiques de configurer et d'appliquer des paramètres de sécurité,
- Veille à ce que les développeurs et leurs conteneurs ne puissent ni assouplir, ni contourner ces paramètres (volontairement ou accidentellement)
- Renforce l'isolation des conteneurs pour empêcher les charges utiles malveillantes de pénétrer dans l'instance virtuelle Linux Docker Desktop et de se propager dans l'hôte sous-jacent.

Fonctionnalités Hardened Docker Desktop, pour protéger l'espace de travail de chaque développeur

Gestion des paramètres

Les administrateurs et les ingénieurs de plateformes peuvent centraliser le contrôle des postes de travail de développeurs : ils prédéfinissent et verrouillent les configurations de leur choix, dans toutes les instances de Docker Desktop.

Seuls les administrateurs informatiques/systèmes possèdent des droits d'administration sur le poste de travail du développeur.

Isolation améliorée des conteneurs

Sécurisez vos conteneurs au sein de l'instance virtuelle (VM) Linux Docker Desktop. Avec ECI, tous les conteneurs sont sans racine (rootless) et ne peuvent pas accéder à la VM Linux ni au moteur Docker qu'elle contient.

Vous évitez ainsi les intrusions, le contournement des configurations et l'accès aux données sensibles stockées à l'intérieur de la VM.

Gestion des accès aux registres

Choisissez les registres auxquels les développeurs peuvent accéder pour introduire ou extraire des artefacts.

Cette fonctionnalité réduit considérablement le risque qu'une image de conteneur contenant des logiciels malveillants ou une image corrompue soit utilisée par vos développeurs.

Gestion des accès aux images

Choisissez les images que les développeurs peuvent extraire de Docker Hub. Sur cette plateforme, se trouvent les images officielles de Docker, les images d'éditeurs vérifiés par Docker et les images Open Source sponsorisées par Docker.

Cette fonctionnalité réduit les risques d'utilisation d'images de conteneurs compromises ou corrompues par les développeurs.

Protégez votre chaîne d'approvisionnement et l'intégrité de vos logiciels : sécurisez les premières étapes du développement logiciel pour que les menaces provenant de logiciels malveillants, de la chaîne d'approvisionnement, de configurations erronées et de collaborateurs malveillants ne puissent pas se propager au-delà de la VM Linux, vers l'hôte natif ou le réseau de l'entreprise.

Faites gagner du temps aux développeurs : définissez des paramètres pour les équipes de développeurs, afin qu'ils puissent se concentrer sur leur cœur de métier : écrire du code.

Gagnez en tranquillité : protégez votre entreprise contre les conséquences catastrophiques d'une attaque de la chaîne d'approvisionnement (pertes financières, problèmes juridiques, atteinte à la réputation, etc.).

Franchissez le pas

Hardened Docker Desktop est déjà disponible avec un abonnement Docker Business.
Il existe quelques conditions préalables à son implémentation.

- Télécharger Docker Desktop 4.13 ou supérieur
- Les administrateurs doivent configurer un registry.json car les utilisateurs doivent être authentifiés pour utiliser ces fonctionnalités.

Pour en savoir plus, consultez notre documentation :

Contactez Nuaware pour en savoir plus sur Hardened Docker Desktop.