GUARDLAB

GL écran

Station blanche GuardLab

La sécurité accessible pour tous

La station blanche offre une réponse adaptée aux menaces USB en servant de point d'entrée unique et contrôlé pour tous les supports tiers.

CONÇU EN FRANCE



Fonctionnalités

La solution est couplée à une API et à un dashboard d'administration permettant aux clients d'administrer et de configurer certaines parties de l'application, mais également de superviser les différentes stations blanches en leur possession.

Détection automatique de périphériques USB

Lorsqu'un périphérique est détecté, l'application récupère ses informations hardware (marque, numéro de série, ...) qui sont remontées dans les logs.

Scan antivirus

Lancement de scans pour chacun des antivirus activés sur la station GuardLab, en simultané. Les résultats sont affichés à l'écran et transmis à le console d'admin.

Fonctionnement hors ligne

Les requêtes qui ne peuvent pas être envoyées à cause du manque de connexion sont stockées jusqu'à ce qu'une nouvelle connexion soit établie.

Multilingue

Anglais.

Mise en veille automatique

GuardLab a la possibilité de mettre en veille ses stations sur des plages horaires définies dans le dashboard d'administration.

Mise à jour automatique

Les mises à jour sont téléchargées en tâche de fond, permettant à l'utilisateur de continuer à utiliser la station. Une fois téléchargée, l'application va redémarrer avec les nouveautés apportées par la mise à jour.

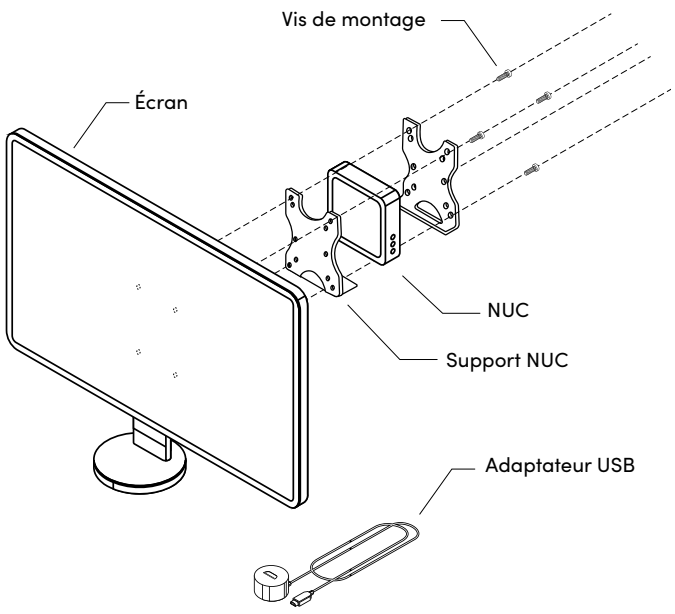
Mise à jour des bases virales

Si une ou plusieurs bases virales ne sont pas à jour, l'application va lancer le script permettant de les mettre à jour.

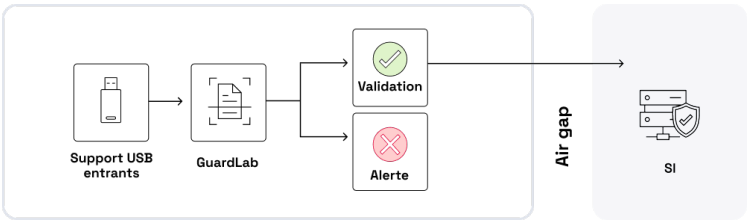
Projet cofinancé par la région Occitanie et l'État dans la cadre du projet France 2030, et opéré par BPI France.

Composition

La station GuardLab écran est adaptée aux budgets restraints, mais qui doivent faire face aux risques d'attaques malveillantes. Composée d'un écran et d'un NUC, elle pourra facilement se positionner dans un coin de bureau.



Architecture



Notre station blanche apporte un point de contrôle dédié, indépendant du système d'information, permettant d'analyser les supports et fichiers entrants avant toute introduction dans le SI. Elle s'intègre dans une démarche de défense en profondeur, en complément des antivirus et solutions de sécurité existantes.

Maîtrise des risques
Réduction de la surface d'attaque liée aux supports amovibles et flux entrants

Continuité de service
Journalisation des analyses, auditabilité des contrôles

Conformité et traçabilité
Limitation des impacts liés aux ransomwares et incidents cyber

Caractéristiques

- Ports USB
- 3 antivirus : With secure, ClamAV, Eset
- Moteur cœur en C++
- Virtualisation
- Fingerprinting (empreintes uniques)
- Durcissement de l'OS et sécurité physique
- Snapshot antivirus via repository
- Communication inter-VM par agent C++ & RabbitMQ
- Architecture ouverte via RabbitMQ
- Architecture virtualisée : offrant une meilleure isolation et une évolutivité pour intégrer de nouveaux moteurs de détection
- Station blanche 100 % logicielle
- Logique d'industrie 4.0 de la cybersécurité

GUARDLAB

contact@humansconnexion.com
www.guardlab.fr