PHIKER
FRANCE

USB SHIELD

PHIKER CORE
POWERED

Sas antimalware de transfert de données
par USB et d'analyse de supports.

PHIKER
FRANCE

MAÎTRISER LA SÉCURITÉ DE VOS FLUX DE DONNÉES DÉCONNECTÉS.

La borne **USB SHIELD** se caractérise par sa taille et son design unique afin de favoriser l'acceptation des utilisateurs. Ceux-ci l'utilisent pour analyser leurs périphériques de stockage USB, mais aussi transférer des données d'un périphérique vers un autre dans un cadre sécurisé.

USB SHIELD est la seule solution proposant l'impression d'un rapport d'activité permettant à l'utilisateur de justifier l'innocuité de l'utilisation d'une clé USB sur un système sensible.

FONCTIONNEMENT DE USB SHIELD

La station est axée sur la sécurisation des données transitant via des périphériques USB.

L'utilisateur peut effectuer une analyse antivirale approfondie, transférer en toute sécurité des données d'un périphérique vers un autre, mais aussi vérifier l'intégrité physique de sa clé et vérifier son espace réel, la reformater ou visualiser le contenu des fichiers.

Un rapport d'activité peut être imprimé, offrant une traçabilité à l'utilisateur.

SÉCURITÉ & SIMPLICITÉ

L'interface graphique a été conçue selon les normes en vigueur d'ergonomie afin de permettre aux utilisateurs une utilisation intuitive. Ainsi sa mise en service ne nécessite pas de formation des utilisateurs. Son format et son design facilitent la conduite du changement en rendant la borne attractive.

Le système s'appuie sur **USB SHIELD OS** de base Linux avec, entre autres, l'utilisation d' USB Guard afin de garantir l'innocuité de la borne dans le temps.

La conception d'**USB SHIELD** respecte le livre blanc de l'ANSSI « sas et station blanche » assurant une protection conforme aux normes les plus rigoureuses en matière de sécurité des données.

POURQUOI CHOISIR USB SHIELD ?

- **Sécurité maximale :** Détection et neutralisation des menaces sur les clés USB.
- **Simplicité et efficacité :** Utilisation conforme et transfert sécurisé entre deux clés.
- **Fonctionnement hors-ligne :** Fonctionnement déconnecté possible avec mise à jour de la base antivirale par clé USB.

Nos solutions hautement sécurisées
s'adaptent à vos spécificités et à vos besoins.

USB SHIELD

Sas antimalware de transfert de données par USB et d'analyse de supports.

*Fonctionne avec **PHIKER CORE***

USB SHIELD se distingue par ses fonctionnalités avancées et son ergonomie pensée pour une utilisation intuitive et efficace :

FONCTIONNALITÉS

- ☑ Analyse anti-virus
- ☑ Vérification d'intégrité
- ☑ Transferts sécurisés de fichiers
- ☑ Impression papier du rapport d'activité
- ☑ Formatage des clés USB compatible Windows/Linux

CONFIGURATION ET MAINTENANCE

- ☑ Livrée prête à poser
- ☑ Mises à jour antivirus rapides et faciles

ADMINISTRATION

- ☑ Fine-tuning du moteur antivirus
- ☑ Possibilité d'associer les bornes à un gestionnaire centralisé (**USB SHIELD MANAGER**)

TRAÇABILITÉ

- ☑ Impression du rapport d'activité
- ☑ Export des logs
- ☑ Export CSV des activités
- ☑ Rapport complet des connexions utilisateurs
- ☑ Lecteur badge en option

ERGONOMIE

- ☑ Interface intuitive et attractive
- ☑ Simplicité d'utilisation

« Avec USB SHIELD, renforcez la sécurité, simplifiez vos transferts de données et gagnez en traçabilité tout en optimisant la gestion de vos périphériques USB. »

EXEMPLE D'UTILISATIONS DE LA SOLUTION USB SHIELD

ANALYSE DE CLÉ USB

Un prestataire insère sa clé USB dans la borne et sélectionne dans le menu «Analyse de la clé» dans le menu. Si une menace est détectée, une alerte visuelle et sonore l'informe.

Plusieurs options s'offrent à lui :

- Formater la clé pour supprimer les menaces
- Transférer les fichiers non contaminés sur une clé saine
- Supprimer la menace

Un rapport d'activité imprimable fournit un récapitulatif des actions et vérifications effectuées.

TRANSFERTS DE FICHIERS

Un consultant souhaitant transférer des fichiers à l'entreprise utilise le premier port USB sur la borne, et l'entreprise le deuxième port USB.

Le consultant lance le transfert des fichiers choisis.

La borne effectue une analyse antivirale complète des fichiers sélectionnés. Si aucune menace n'est détectée, la copie est alors initiée. Un système unique de purge des tampons permet de garantir que la copie soit complète et effective sur la clé de destination.

À la fin du transfert, un rapport d'activité imprimable atteste de la sécurité des fichiers contrôlés ainsi que du bon déroulement des opérations.

RÉALITÉ DU TERRAIN

Malgré des efforts considérables, la majorité des entreprises n'a pas réussi à éliminer complètement les flux de données déconnectés.

En 2023, Honeywell Forge estimait que 37% des menaces étaient conçues spécifiquement pour une propagation par USB, et que 79% avaient pour cible les technologies opérationnelles. Ainsi, un seul fichier peut détruire des outils de valeurs, chiffrer ou altérer des données sensibles, handicapant drastiquement la production. Il suffit qu'une seule de ces menaces soit filtrée par **USB SHIELD** pour que le retour sur investissement soit largement positif.

Le sas **USB SHIELD** permet de s'adapter à la réalité du terrain en proposant un format, un design et une ergonomie facilitant la sensibilisation et l'acceptation du personnel à cette réalité.

Ainsi, **USB SHIELD** vous permet d'éliminer la menace USB en garantissant l'innocuité des clés USB.

AUDIT ■ CONCEPTION ■ MATÉRIALISATION ■ DÉPLOIEMENT ■ MAINTENANCE ■ DÉPANNAGE

+33(0)4 22 46 01 95
11, chemin de l'industrie • Nodelys
06110 LE CANNET

PHIKER
FRANCE
www.phiker.fr

TARIFS

	Prix HT
BORNE	**5 000 €**
LICENCE Par an et par borne, inclut les licences des antivirus	**850 €**
PERSONNALISATION AUX COULEURS ET LOGO DE VOTRE ENTREPRISE Hors MCO	**3 000 €**
FORMATION DES ADMINISTRATEURS ET UTILISATEURS Une demi-journée en webinaire	**600 €**
PERSONNALISATION SUR-MESURE	**Sur devis**
FLOCAGE SUR-MESURE	**Sur devis**
AJOUT ET/OU MODIFICATION DE FONCTIONNALITÉS Hors MCO/MCS	**Sur devis**

+33(0)4 22 46 01 95
contact@phiker.fr
11, chemin de l'industrie • Nodelys
06110 LE CANNET

PHIKER
FRANCE
www.phiker.fr