BLACK BOX®

BROCHURE
KVM SÉCURISÉ

Secure KVM Switches

Brochure sur les solutions

EN SAVOIR PLUS BLACKBOX.COM/SECUREKVM

Combattre les diverses menaces de sécurité qui se posent lors du partage de périphériques entre des réseaux informatiques ayant des niveaux de sécurité différents

Pourquoi Secure KVM ?

Les cybermenaces évoluent constamment, devenant chaque jour plus fréquentes et plus sophistiquées. Notre dépendance à l'égard de la technologie, le partage des ressources mondiales et la nécessité d'une collaboration en temps réel ont donné naissance à un réseau de données de plus en plus vaste. Si l'interconnectivité nous aide à travailler ensemble de manière plus efficace, elle nous rend aussi de plus en plus vulnérables à des cyberattaques dévastatrices.

Les grandes agences de défense et d'autres organisations utilisent des mesures de sécurité avancées pour isoler les réseaux et protéger les informations contre les menaces extérieures. Cependant, il existe un endroit où les réseaux isolés et les informations sensibles se rencontrent : le bureau de l'utilisateur.

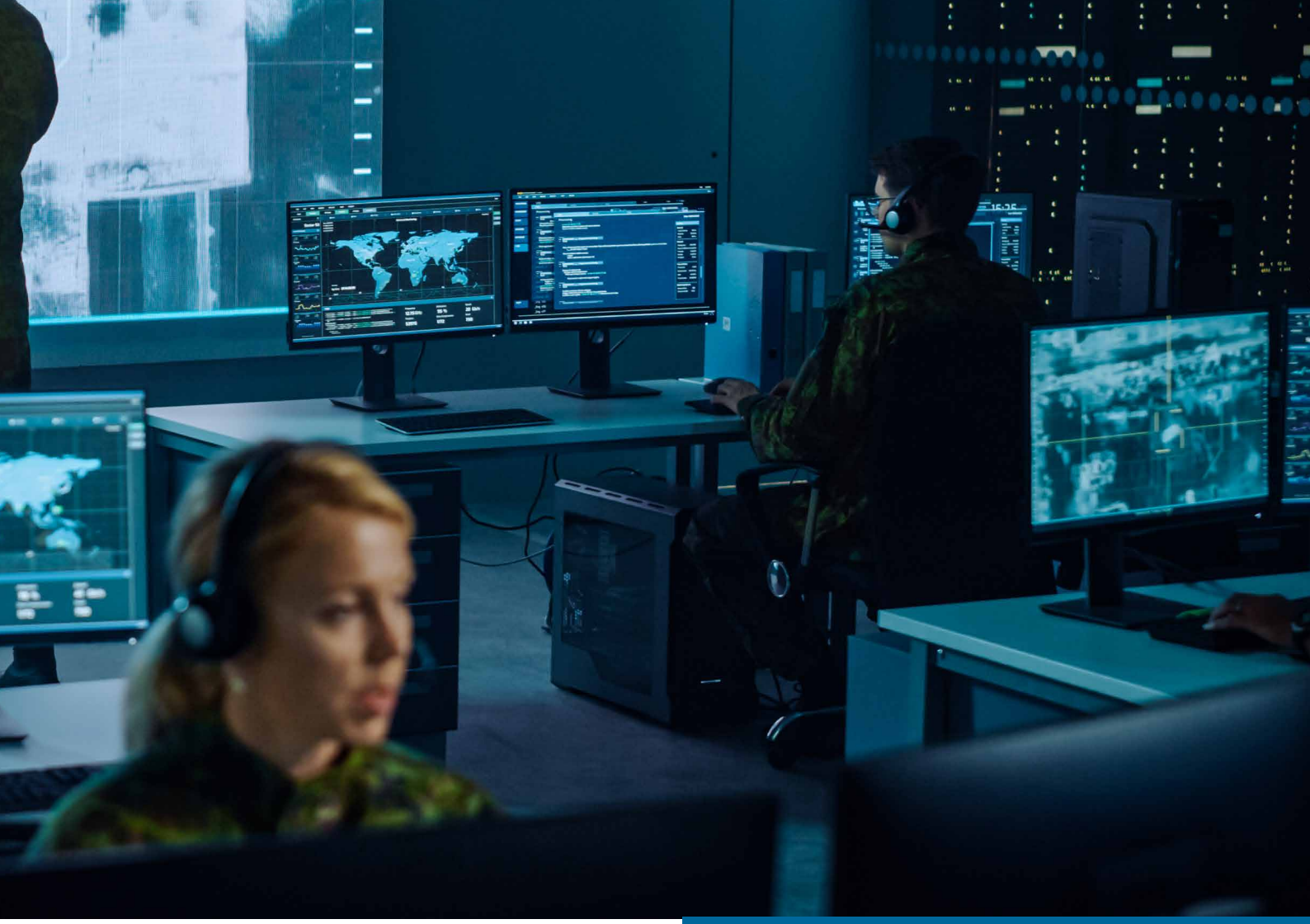
Les commutateurs KVM non sécurisés sont susceptibles de faire l'objet de cyberattaques et peuvent permettre aux cybercriminels d'accéder à des données classifiées. Si un cybercriminel veut voler des informations sur un serveur classifié, il peut attacher une clé USB contenant des logiciels malveillants ou un virus à un commutateur KVM non sécurisé pour accéder à plusieurs serveurs au lieu d'un seul. Les commutateurs KVM non sécurisés sont également susceptibles de faire l'objet d'une utilisation malveillante des écrans LCD (via le signal EDID), des microphones ou des dispositifs CAC.

Ces méthodes permettent à une multitude d'informations classifiées de tomber entre de mauvaises mains et d'être utilisées pour nuire à l'organisation.

Commutateurs KVM traditionnels

Les commutateurs KVM permettent d'accéder à plusieurs ordinateurs et de les gérer à partir d'un seul poste de travail à l'aide d'un clavier, d'une souris et d'un écran vidéo. Les utilisateurs peuvent facilement accéder à des informations et à des applications sur des systèmes complètement séparés en appuyant sur un bouton ou en utilisant des touches.

La technologie KVM fournit des solutions de surveillance pour l'automatisation, les processus et les flux de travail. Il offre aux utilisateurs une meilleure opérabilité et un retour sur investissement rapide grâce à l'amélioration de l'ergonomie et de la productivité sur le lieu de travail. Les commutateurs KVM permettent aux utilisateurs de gagner de l'espace en réduisant le nombre de dispositifs d'interface, de réduire les coûts en éliminant les périphériques redondants et de réagir plus rapidement dans les situations critiques.



Les commutateurs KVM sécurisés préservent la confidentialité des données sensibles

Un commutateur KVM sécurisé est un commutateur de bureau à 2, 4 ou 8 ports qui permet de contrôler et de séparer les PC connectés à des réseaux de différentes classifications de sécurité. Contrairement aux commutateurs KVM traditionnels, les commutateurs KVM sécurisés ne peuvent être contrôlés qu'à l'aide d'un bouton-poussoir. Les commandes par raccourci clavier sont désactivées, ce qui garantit que seuls les bons utilisateurs y ont accès.

Les commutateurs KVM sécurisés ne permettent pas à une clé USB non reconnue d'accéder à des informations. Il permet aux administrateurs de choisir quels périphériques USB sont autorisés ou reconnus. Les commutateurs KVM sécurisés font beaucoup, beaucoup plus pour protéger les agences gouvernementales contre les cybermenaces les plus terrifiantes d'aujourd'hui.

Profil de protection NIAP pour KVM sécurisé

Jusqu'à récemment, le National Information Assurance Partnership (NIAP) utilisait le Common Criteria Evaluation & Validation Scheme (CCEVS) pour évaluer et approuver la sécurité des commutateurs KVM.

La NIAP a mis en œuvre la déclaration de vision du comité de gestion de l'Arrangement de reconnaissance des critères communs (ADRC) pour l'application des critères communs et n'évalue plus les niveaux d'assurance de l'évaluation (EAL). Cela permet de renforcer les évaluations en se concentrant sur les exigences de sécurité spécifiques à la technologie.

En conséquence, ils ont mis à jour le profil de protection (PP) pour les commutateurs de partage de périphériques en PP 4.0 NIAP Protection Profile for Peripheral Sharing Switch Version 4.0, qui sont des tests concernant le processus de conception, de test, de vérification et d'expédition des produits de sécurité. Ce profil de protection est un processus international normalisé d'évaluation, de validation et de certification de la sécurité des technologies de l'information.

Comment les commutateurs KVM sécurisés luttent contre les cyberattaques

Caractéristiques de sécurité rigides à l'intérieur des commutateurs KVM sécurisés de Black Box

- L'isolation mécanique, électrique et optique des signaux empêche le piratage et la fuite de données -> isolation absolue / pas de fuite de données entre les ports sécurisés et le monde extérieur
- Le micrologiciel protégé empêche les intrus de reprogrammer ou de lire le micrologiciel (ROM non reprogrammable).
- Les ports USB opto-isolés et l'effacement du cache clavier interne maintiennent les chemins de données USB électriquement isolés les uns des autres afin d'éviter les fuites de données entre les ports USB.
- L'émulation EDID/vidéo et aux sécurisée limite la découverte des écrans nouvellement connectés lors des opérations de commutation, ce qui empêche la transmission de données indésirables et non sécurisées entre les ordinateurs et l'écran.
- Protection du châssis contre les intrusions : équipé de commutateurs actifs anti-sabotage et de scellés anti-sabotage à hologramme externe.
- Carte d'accès commune (CAC) configurable en option pour les cartes à puce, les lecteurs biométriques et l'enregistrement des périphériques USB externes.
- Flux de données unidirectionnel vers des périphériques spéciaux tels qu'un projecteur, une imprimante ou un système audio
- Certifié NIAP PP 4.0, le niveau le plus élevé des critères communs (profil de protection pour le commutateur de partage de périphériques version 4.0).
- Conforme à la loi TAA et fabriqué aux États-Unis
- L'entrée audio est autorisée, mais uniquement si aucun autre type de périphérique n'est pris en charge par le commutateur (le microphone ne peut pas coexister avec les haut-parleurs).

Testé et certifié selon le dernier profil de sécurité NIAP PP 4.0

Les commutateurs KVM sécurisés de Black Box sont conçus pour être utilisés dans des applications sécurisées de défense et de renseignement où des données sensibles doivent être protégées. Les commutateurs KVM sécurisés de Black Box sont certifiés NIAP PP 4.0 et dotés des fonctions de sécurité les plus élevées qui répondent aux normes actuelles de contrôle de l'assurance de l'information. Les commutateurs contiennent des configurations matérielles uniques qui empêchent la fuite de données entre les PC et les périphériques connectés, éliminant ainsi toute cybermenace potentielle. NIAP PP 4.0 applique un profil de protection de base avec des modules individuels pour les types de périphériques.

Sécurité à plusieurs niveaux pour une assurance stricte de l'information

L'isolation absolue des signaux mécaniques, électriques et optiques grâce à l'étanchéité à l'air empêche le piratage et la fuite de données entre les ports et le monde extérieur. Chaque port du commutateur KVM sécurisé utilise ses propres canaux de données isolés. En allumant d'emblée un autre ordinateur cible, le commutateur KVM efface le cache interne et les données du clavier pour s'assurer qu'aucune donnée résiduelle ne subsiste dans le canal. Le micrologiciel et la ROM fixes et sécurisés ne sont pas reprogrammables et empêchent les intrus de lire, de reprogrammer par des mises à jour non souhaitées du micrologiciel ou de supprimer physiquement des données sensibles.

Protection contre les intrusions dans le châssis

Les commutateurs KVM sécurisés sont dotés de commutateurs actifs et anti-sabotage, scellés avec hologramme externe d'inviolabilité et d'une batterie interne anti-sabotage à longue durée de vie. Si le couvercle est retiré du châssis, le commutateur KVM coupe la connexion avec tous les PC et périphériques connectés et désactive toute fonctionnalité afin de se protéger contre toute tentative d'intrusion physique. La réponse à l'autoprotection est facultative dans la version 4.0 (elle est obligatoire dans la version 3.0), car certains dispositifs peuvent avoir des cartes interchangeables pour différents types de périphériques (auquel cas les scellés d'autoprotection sont suffisants). La version 3.0 interdit l'entrée audio (microphone), tandis que la version 4.0 autorise l'entrée audio (mais uniquement si l'appareil ne prend pas en charge d'autres types de périphériques ; par exemple, un microphone ne peut pas coexister avec des haut-parleurs).

Émulation du clavier et de la souris

Le commutateur KVM sécurisé émule la présence d'un clavier et d'une souris pour chaque ordinateur connecté via un câble USB. Les ordinateurs sélectionnés et non sélectionnés maintiennent une connexion constante avec les contrôleurs d'émulation de clavier et de souris du commutateur, ce qui permet une commutation ultra-rapide et limite la découverte de périphériques nouvellement connectés pendant les opérations de commutation. L'émulation du clavier et de la souris empêche également la connexion directe entre les périphériques et les ordinateurs connectés, protégeant ainsi les systèmes des vulnérabilités potentielles. Les ports PS/2 sont autorisés dans la version 3.0 et sont interdits dans la version 4.0.

Port Common Access Card (CAC) entièrement configurable pour les périphériques USB externes

De nombreux commutateurs KVM sécurisés prennent en charge les dispositifs CAC (Common Access Card), tels que les lecteurs de cartes à puce et les lecteurs biométriques, ce qui renforce la sécurité lors de l'utilisation de l'appareil. Cependant, Black Box va encore plus loin dans la sécurité CAC en permettant aux administrateurs authentifiés d'enregistrer et d'affecter des périphériques spécifiques au port CAC (en option). Les utilisateurs peuvent alors commuter la connexion entre l'appareil assigné et la commutation KVM des ordinateurs connectés.

Limite les nouvelles connexions de moniteurs pendant la commutation

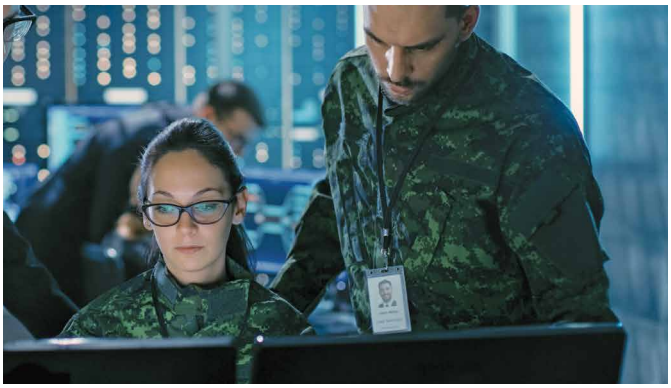
Les commutateurs KVM sécurisés simulent un EDID générique par défaut, ce qui leur permet de faire fonctionner la plupart des moniteurs connectés. Les ordinateurs sélectionnés et non sélectionnés maintiennent une connexion constante avec les contrôleurs d'émulation vidéo et AUX du commutateur, ce qui permet une commutation ultra-rapide et limite la découverte de nouveaux moniteurs connectés pendant les opérations de commutation. Les systèmes sont ainsi protégés contre les vulnérabilités potentielles dues à la transmission de données non désirées et non sécurisées par les lignes DDC. La version 4.0 permet l'utilisation de visionneuses multiples (cependant, elles doivent utiliser l'OSD pour identifier le(s) canal(aux) vidéo actif(s)).

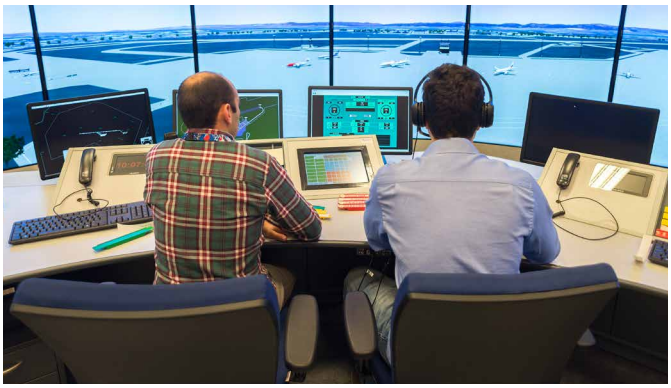
Cas d'utilisation

Idéal pour plusieurs secteurs d'activité

- Gouvernement
- Défense et armée
- Salles de contrôle pour la gestion du trafic
- Banque et finance
- Éducation
- Soins de santé
- Départements de R&D
- Utilitaires

Cas d'utilisation





Centre de communication de la défense

Un client du secteur de la défense s'est adressé à Black Box avec deux problèmes urgents : un accès réseau inefficace et un espace de travail encombré.

Les opérateurs devaient accéder à de multiples réseaux informatiques dans des centres de communication sécurisés. Ce processus prenait beaucoup de temps car chaque réseau informatique nécessitait un clavier, un écran et une souris distincts, ce qui signifiait que l'opérateur devait se déplacer entre les différents systèmes pour accéder aux données sensibles et aux réseaux de renseignement. Il fallait également une table pour les six moniteurs, les six claviers et les six souris, ce qui créait un espace de travail encombré et exigu.

Pour relever ces défis, ils ont acheté un commutateur KVM sécurisé à 8 ports de Black Box qui a réduit leur configuration à un seul moniteur, un seul clavier et une seule souris, ce qui a permis aux opérateurs de gagner un temps précieux en devant basculer entre plusieurs réseaux et a libéré beaucoup d'espace sur les bureaux. Désormais, ils travaillent plus efficacement dans un espace de travail propre tout en s'assurant que leurs données vitales ne risquent pas d'être compromises.

Police

Une entreprise a contacté Black Box pour une solution hautement sécurisée pour un projet police. Les ingénieurs du projet devaient passer d'un réseau ouvert (vert) à un réseau sécurisé (rouge). Black Box a suggéré le commutateur KVM sécurisé DVI USB à 4 ports, qui répond parfaitement à toutes leurs exigences. Plus de 1 000 commutateurs KVM sécurisés ont déjà été installés.

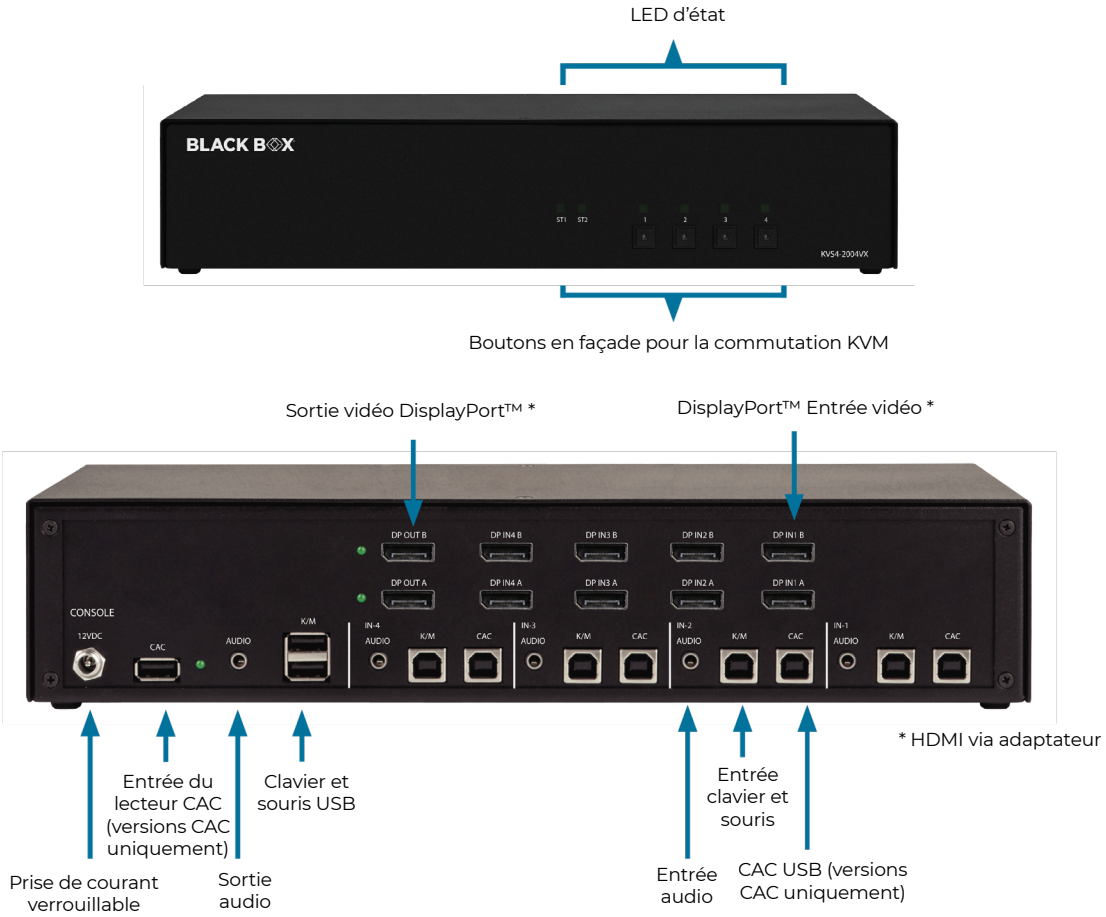
Entreprise

Le partage des ressources mondiales et la nécessité d'une collaboration en temps réel ont donné naissance à un réseau de données de plus en plus vaste. Si l'interconnectivité permet aux organisations de travailler ensemble de manière plus efficace, elle les rend également de plus en plus vulnérables à des cyberattaques dévastatrices. Enfin, les systèmes qui accèdent à l'internet doivent être tenus à l'écart des autres systèmes utilisés pour les données sensibles de l'entreprise ou les données personnelles. Pour maintenir l'assurance de leurs informations, de nombreuses organisations remplacent les commutateurs KVM standard par des commutateurs KVM sécurisés.

Présentation du produit Secure KVM

Conception d'un commutateur KVM sécurisé

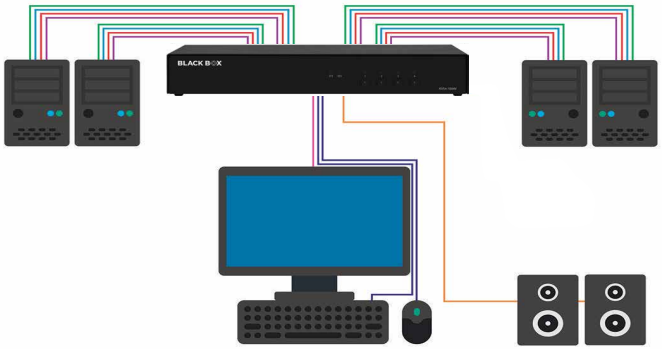
Exemple Commutateur KVM sécurisé à 4 ports, un seul utilisateur, DisplayPort, USB et CAC KVS4-2004VX



Types de commutateurs KVM de bureau sécurisés certifiés NIAP 4.0

Commutateurs KVM de bureau sécurisés, mono-utilisateur

- Partage d'une console utilisateur unique entre deux, quatre ou huit ordinateurs
- Disponible avec vidéo DVI-I, DisplayPort ou HDMI/ DisplayPort
- Vidéo DisplayPort 1.2/HDMI de haute qualité avec des résolutions jusqu'à 4K@60Hz et meilleure résolution DVI-I dual-link jusqu'à 2560x1600 @ 60Hz
- Choisissez parmi les modèles avec connexion à un, deux ou quatre moniteurs à la console.
- Clavier/souris USB et audio stéréo
- Disponible avec ou sans support CAC
- Fabriqué, testé et certifié aux États-Unis



Trouvez le bon produit dans le sélecteur des pages 11 et 12.

Contrôleur KVM sécurisé

Contrôleur de bouton-poussoir KVM sécurisé

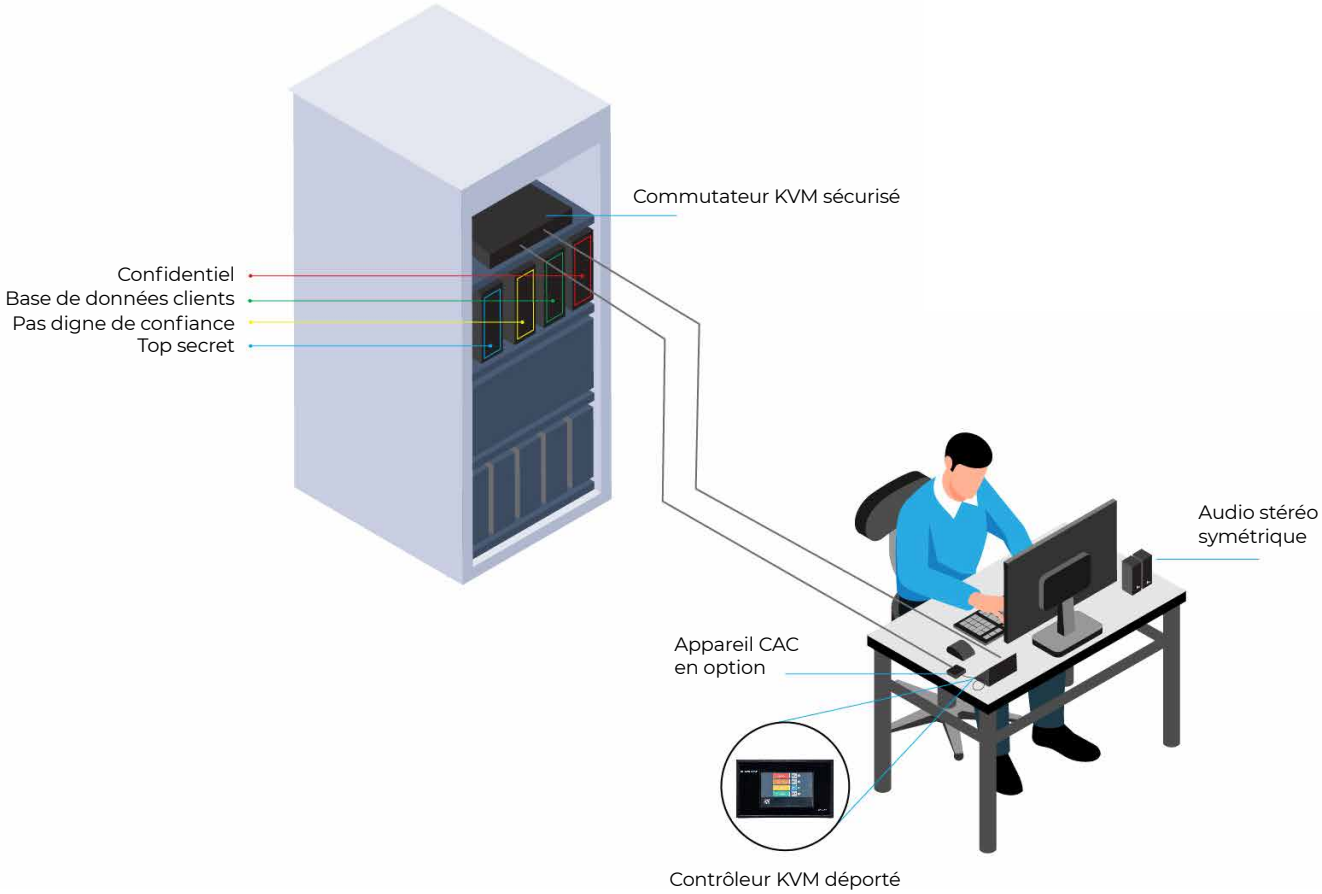
- Commutation entre des réseaux classifiés, strictement confidentiels et ouverts, le commutateur KVM certifié NIAP4 ne devant pas rester sur le bureau.
- Contrôle les commutateurs KVM sécurisés à 2 et 4 ports via un seul câble USB
- Prend en charge la commutation CAC jusqu'à une distance de 9 m du commutateur

Contrôleur de bouton-poussoir KVM sécurisé KVSC-4

Contrôleur d'écran tactile KVM sécurisé

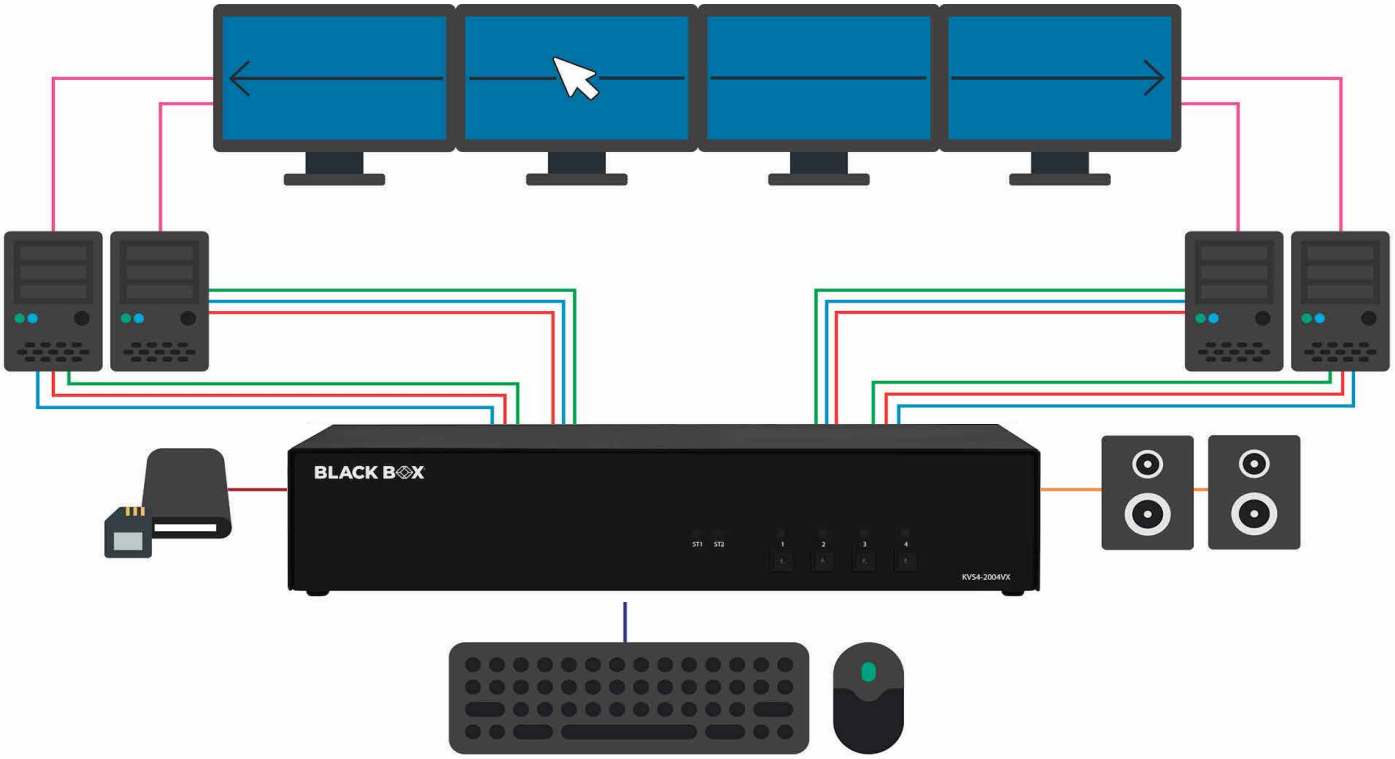
- Détection automatique de jusqu'à 16 connexions
- L'écran tactile LCD couleur rétroéclairé offre une vue d'ensemble claire et cristalline des appareils connectés
- Prend en charge la commutation du clavier et de la souris jusqu'à une distance de 15 mètres du commutateur
- Prêt pour l'avenir : cette solution de câble USB unique prend en charge votre système maintenant et plus tard, au fur et à mesure de sa croissance

Écran tactile KVM sécurisé - ContrôleurKVSC-16



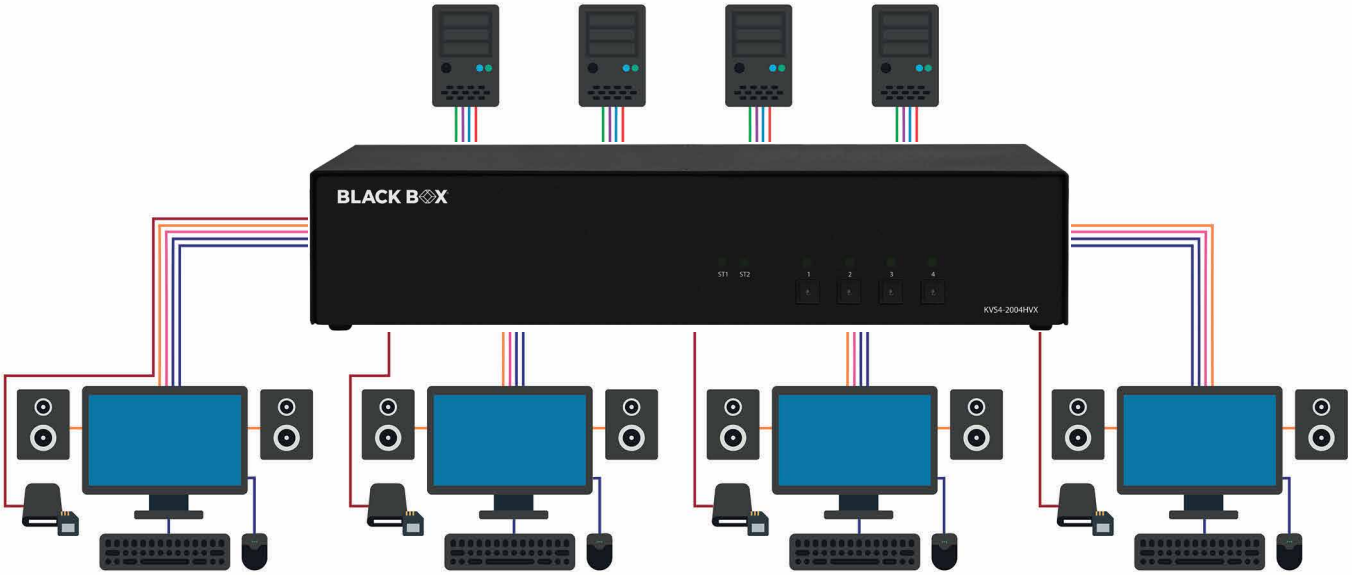
Commutateurs KM sécurisés certifiés NIAP 4.0

- Passer d'un écran à l'autre en déplaçant la souris (Glide & Switch)
- Visualisation simultanée de plusieurs sources grâce à des connexions ordinateur/moniteur dédiées
- Prise en charge de l'audio stéréo
- Partage d'une console utilisateur unique avec clavier et souris USB entre quatre ou huit ordinateurs
- Prise en charge de l'audio stéréo
- Disponible avec ou sans support CAC
- Fabriqué, testé et certifié aux États-Unis



Commutateur KVM sécurisé certifié NIAP 4.0 - FlexPort HDMI/DisplayPort

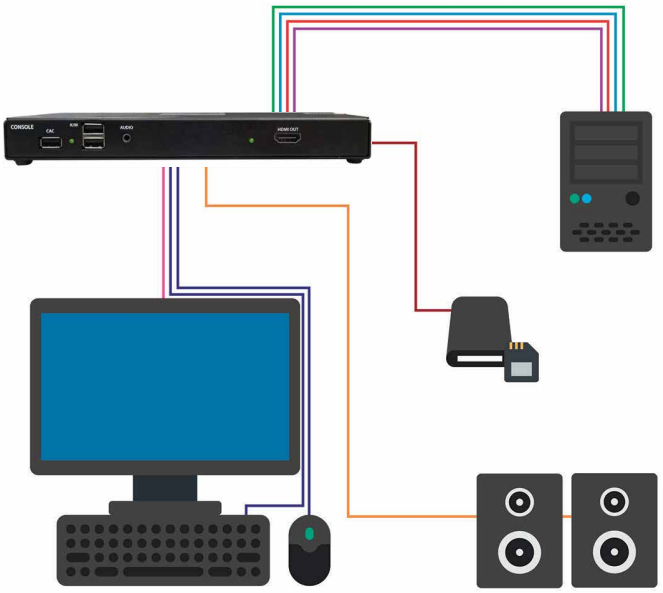
- Fonctionnement sécurisé du clavier, de la vidéo et de la souris sur un maximum de deux ou quatre ordinateurs avec un ou deux moniteurs HDMI/DisplayPort utilisant la technologie FlexPort
- Certifié pour le NIAP Protection Profile for Peripheral Sharing Device Version 4.0
- Prend en charge les résolutions jusqu'à 4K@60Hz
- Fabriqué, testé et certifié aux États-Unis
- Alimentation électrique externe



Trouvez le bon produit dans le sélecteur des pages 11 et 12.

Secure KVM Peripheral Defender, certifié NIAP 4.0 - CAC

- Isole un ordinateur du moniteur DVI-I, HDMI ou DisplayPort, du clavier, de la souris et du CAC pour garantir la sécurité.
- Certifié pour le NIAP Protection Profile for Peripheral Sharing Device Version 4.0
- Interface vidéo à moniteur unique
- Protection des périphériques non sécurisés
- Testé et certifié dans le cadre du programme américain
- Alimentation électrique externe
- Assure un flux de données unidirectionnel de la vidéo, de l'USB et de l'audio de l'ordinateur vers le périphérique.
- Prise en charge de la plupart des moniteurs grâce à l'apprentissage/émulation EDID sécurisée
- Idéal pour les salles de conférence afin de protéger les ordinateurs portables contre les intrusions par le biais de la connexion d'affichage partagée.



Trouvez le bon produit dans le sélecteur des pages 11 et 12.

SOLUTIONS DE PRODUITS NIAP 4.0					
COMMUTATEUR KVM SÉCURISÉ, CERTIFIÉ NIAP 4.0, DISPLAYPORT					
ARTICLE #	KVS4-1004V	KVS4-2002V	KVS4-2004V	KVS4-2004VX	KVS4-2008VX
La description	2 ports, moniteur unique, DisplayPort	2 ports, double moniteur, DisplayPort	4 ports, double moniteur, DisplayPort	4 ports, double moniteur, DisplayPort, CAC	8 ports, double moniteur, DisplayPort, CAC
Nombre de sources	2	2	4	4	8
Compatibilité informatique	Windows®, Mac®, et Linux® OS				
Max. Résolution	Jusqu'à 4K@60Hz				
Compatibilité des moniteurs	La plupart des moniteurs grâce à l'apprentissage et à l'émulation EDID sécurisés				
PORTS VERS LA CONSOLE UTILISATEUR					
Connexion(s) au moniteur	(1) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort
Connexions clavier/souris	(2) USB 2.0 Type A, clavier et souris uniquement				
Sortie audio	(1) Prise audio 3,5 mm avec sorties haut-parleurs symétriques et commutation				
CAC supporté	Non	Non	Non	(1) USB Type A, entièrement configurable	(1) USB Type A, entièrement configurable
PORTS VERS LES ORDINATEURS					
Connexion(s) au moniteur	(1) DisplayPort par source	(2) DisplayPort par source	(2) DisplayPort par source	(2) DisplayPort par source	(2) DisplayPort par source
Connexions clavier/souris	(1) USB 2.0 Type B avec émulation USB par source				
Sortie audio	(1) Prise audio de 3,5 mm par source				
CAC supporté	Non	Non	Non	(1) USB Type B par source	(1) USB Type B par source

COMMUTATEUR KVM SÉCURISÉ, CERTIFIÉ NIAP 4.0, DVI-D					
ARTICLE #	KVS4-1002D	KVS4-1004D	KVS4-2002D	KVS4-2004D	KVS4-2008D
La description	4 ports, moniteur unique, DVI-D	4 ports, moniteur unique, DVI-D	2 ports, double moniteur, DVI-D	4 ports, double moniteur, DVI-D	8 ports, double moniteur, DVI-D
Nombre de sources	4	4	2	4	8
Compatibilité informatique	Windows®, Mac®, et Linux® OS				
Max. Résolution	2560 x 1600 à 60 Hz				
Compatibilité des moniteurs	La plupart des moniteurs grâce à l'apprentissage et à l'émulation EDID sécurisés				
PORTS VERS LA CONSOLE UTILISATEUR					
Connexion(s) au moniteur	(1) DVI-D	(1) DVI-D	(2) DVI-D	(2) DVI-D	(2) DVI-D
Connexions clavier/souris	(2) USB 2.0 Type A, clavier et souris uniquement				
Sortie audio	(1) Prise audio 3,5 mm avec sorties haut-parleurs symétriques et commutation				
CAC supporté	Non	Non	Non	Non	Non
PORTS VERS LES ORDINATEURS					
Entrée(s) vidéo	(1) DVI-D par source	(1) DVI-D par source	(2) DVI-D par source	(2) DVI-D par source	(2) DVI-D par source
Entrées clavier/souris	(1) USB 2.0 Type B avec émulation USB par source				
Sortie audio	(1) Prise audio de 3,5 mm par source				
CAC supporté	Non	Non	Non	Non	Non

COMMUTATEUR KVM SÉCURISÉ, CERTIFIÉ NIAP 4.0, FLEXPORT HDMI/DISPLAYPORT				
Article #	KVS4-1004HV	KVS4-2002HV	KVS4-2004HV	KVS4-2004HVX
La description	4 ports, moniteur unique, FlexPort HDMI/DisplayPort	2 ports, double moniteur, FlexPort HDMI/DisplayPort	4 ports, double moniteur, FlexPort HDMI/DisplayPort	4 ports, double moniteur, FlexPort HDMI/DisplayPort, CAC
Nombre de sources	4	2	4	4
Compatibilité informatique	Windows®, Mac®, et Linux® OS			
Max. Résolution	Jusqu'à 4K@60Hz			
Compatibilité des moniteurs	La plupart des moniteurs grâce à l'apprentissage et à l'émulation EDID sécurisés			
PORTS VERS LA CONSOLE UTILISATEUR				
Connexion(s) au moniteur	(1) HDMI/DisplayPort FlexPorts	(2) FlexPorts HDMI/ DisplayPort	(2) FlexPorts HDMI/ DisplayPort	(2) FlexPorts HDMI/ DisplayPort
Connexions clavier/souris	(2) USB 2.0 Type A, clavier et souris uniquement			
Sortie audio	(1) Prise audio 3,5 mm avec sorties haut-parleurs symétriques et commutation			
CAC supporté	Non	Non	Non	(1) USB Type A, entièrement configurable
PORTS VERS LES ORDINATEURS				
Entrée(s) vidéo	(1) FlexPorts HDMI/ DisplayPort par source	(2) FlexPorts HDMI/ DisplayPort par source	(2) FlexPorts HDMI/ DisplayPort par source	(2) FlexPorts HDMI/ DisplayPort par source
Entrées clavier/souris	(1) USB 2.0 Type B avec émulation USB par source			
Sortie audio	(1) Prise audio de 3,5 mm par source			
CAC supporté	Non	Non	Non	(1) USB Type B par source

SECURE KVM PERIPHERAL DEFENDER, CERTIFIÉ NIAP 4.0 - CAC			
Article #	KVS4-8001DX	KVS4-8001HX	KVS4-8001VX
La description	DVI-D, CAC	HDMI, CAC	DisplayPort, CAC
Compatibilité informatique	Windows®, Mac®, et Linux® OS		
Max. Résolution	2560 x 1600 @ 60Hz (DVI-D) Jusqu'à 4K@60Hz (modèles HDMI et DisplayPort)		
Compatibilité des moniteurs	La plupart des moniteurs grâce à l'apprentissage et à l'émulation EDID sécurisés		
PORTS VERS LA CONSOLE UTILISATEUR			
Connexion(s) au moniteur	(1) DVI-D 23 broches (femelle)	(1) HDMI 1.4	(1) DisplayPort
Connexions clavier/souris	(2) USB Type-A pour la connexion du clavier et de la souris uniquement (1) USB Type-A pour la connexion CAC	(2) USB Type-A pour la connexion du clavier et de la souris uniquement (1) USB Type-A pour la connexion CAC	(2) USB Type-A pour la connexion du clavier et de la souris uniquement (1) USB Type-A pour la connexion CAC
Sortie audio	(1) Connecteur stéréo 3,5 mm femelle	(1) Connecteur stéréo 3,5 mm femelle	(1) Connecteur stéréo 3,5 mm femelle
CAC supporté	(1) USB Type A, entièrement configurable	(1) USB Type A, entièrement configurable	(1) USB Type A, entièrement configurable
PORTS VERS LES ORDINATEURS			
Entrée vidéo	(1) DVI-D 23 broches (femelle)	(1) HDMI 1.4	(1) DisplayPort
Entrées clavier/souris	(1) USB Type-B	(1) USB Type-B	(1) USB Type-B
Sortie audio	(1) Connecteur stéréo 3,5 mm femelle	(1) Connecteur stéréo 3,5 mm femelle	(1) Connecteur stéréo 3,5 mm femelle
CAC supporté	(1) USB Type B	(1) USB Type B	(1) USB Type B

BLACK BOX®

Pourquoi Black Box ?

Savoir-faire

Les ingénieurs projet Black Box peuvent contribuer à l'évaluation, à la conception, au déploiement et à la formation du système.

Gamme

Black Box propose la gamme de solutions KVM la plus complète de l'industrie.

Support

Reflétant notre engagement pour une satisfaction totale, notre équipe dédiée de techniciens d'assistance hautement qualifiés est disponible par téléphone gratuitement, tous les jours de l'année.

Garanties

Les commutateurs KVM Secure bénéficient d'une garantie de 3 ans et des options d'extension sont disponibles.

Expérience

Fournisseur de solutions technologiques de pointe depuis 1976, Black Box aide plus de 175 000 clients dans 150 pays à créer, gérer, optimiser et sécuriser des infrastructures informatiques.

Centre d'excellence

Black Box propose un centre d'excellence comprenant des services professionnels et des accords de support qui aident à optimiser les systèmes des clients et à maximiser le temps de fonctionnement.

Accords de Niveau de Service

Nos accords de niveau de service permettent aux clients d'accéder à une assistance technique, à une formation sur les produits, à des ingénieurs d'application dédiés, et bien plus encore.

2024 BLACK BOX CORPORATION. TOUS DROITS RÉSERVÉS.