BLACK BOX®

BROCHURE
TECNOLOGIA KVM

Switch KVM Secure

Opuscolo sulle soluzioni

SCOPRI DI PIÙ BLACKBOX.COM/SECUREKVM

Combatti la varietà di minacce alla sicurezza che si presentano quando si condividono periferiche tra reti di computer con livelli di sicurezza diversi

Perché Secure KVM

Le minacce informatiche sono in continua evoluzione e diventano ogni giorno più frequenti e sofisticate. La nostra dipendenza dalla tecnologia, la condivisione di risorse globali e la necessità di collaborare in tempo reale hanno portato a una crescente rete di dati. Se da un lato l'interconnettività ci aiuta a lavorare insieme in modo più efficiente ed efficace, dall'altro ci rende sempre più vulnerabili a devastanti attacchi informatici.

Le principali agenzie di difesa e altre organizzazioni utilizzano misure di sicurezza avanzate per isolare le reti e proteggere le informazioni dalle minacce esterne. Tuttavia, c'è un luogo in cui reti isolate e informazioni sensibili si incontrano: il desktop dell'utente.

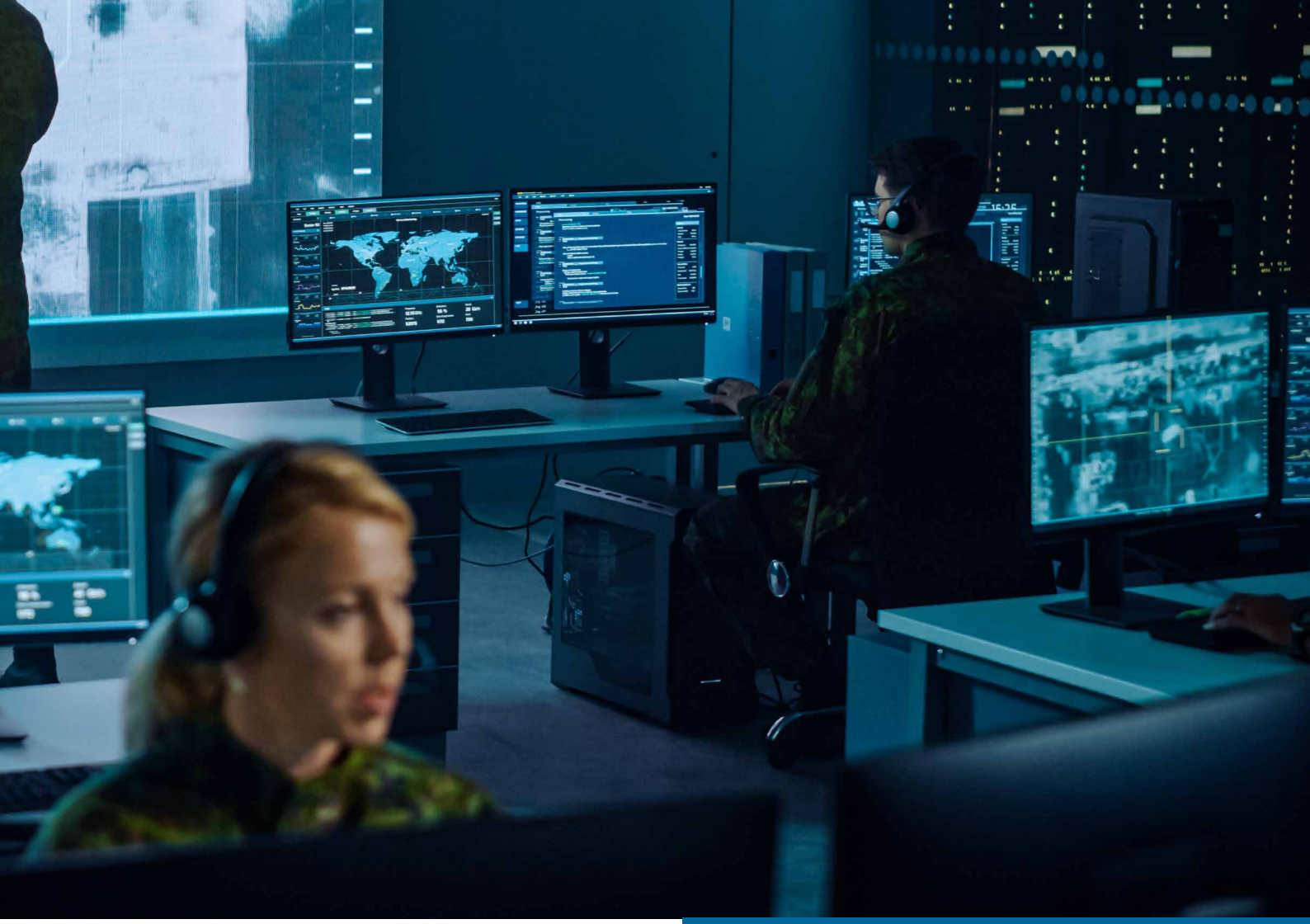
Gli switch KVM non sicuri sono suscettibili di attacchi informatici e possono consentire ai criminali informatici di accedere a dati riservati. Se un criminale informatico vuole rubare informazioni da un server classificato, può collegare un'unità USB contenente malware o virus a uno switch KVM non sicuro per accedere a più server invece che a uno solo. Gli switch KVM non sicuri sono anche suscettibili di un uso malevolo dei monitor LCD (tramite il segnale EDID), dei microfoni o dei dispositivi CAC.

Attraverso questi metodi, una grande quantità di informazioni classificate può finire nelle mani sbagliate ed essere utilizzata per danneggiare l'organizzazione.

Switch KVM tradizionali

Gli switch KVM consentono di accedere e gestire più computer da un'unica postazione di lavoro con tastiera, mouse e monitor. Gli utenti possono accedere facilmente a informazioni e applicazioni su sistemi completamente separati, premendo un pulsante o utilizzando i tasti.

La tecnologia KVM offre soluzioni di monitoraggio per l'automazione, i processi e il flusso di lavoro. Offre agli utenti una migliore operatività e un rapido ritorno sull'investimento grazie alla migliore ergonomia e produttività della postazione di lavoro. Gli switch KVM consentono agli utenti di risparmiare spazio riducendo i dispositivi di interfaccia, di risparmiare sui costi eliminando le periferiche ridondanti e di reagire più rapidamente in situazioni critiche.



Esempi di utilizzo

Gli switch KVM sicuri mantengono i dati sensibili classificati

Uno switch KVM sicuro è uno switch desktop a 2, 4 o 8 porte che consente di controllare e separare i PC collegati a reti con classificazioni di sicurezza diverse. A differenza degli switch KVM tradizionali, gli switch KVM sicuri possono essere controllati solo tramite pulsanti. I comandi di scelta rapida sono disabilitati, in modo da garantire l'accesso solo agli utenti giusti.

Gli switch KVM sicuri non consentono a un'unità USB non riconosciuta di accedere alle informazioni. Consentono agli amministratori di scegliere quali dispositivi USB sono autorizzati o riconosciuti. Gli switch KVM sicuri fanno molto, molto di più per proteggere le agenzie governative dalle minacce informatiche più terrificanti di oggi.

NIAP Protection Profile per Secure KVM

Fino a poco tempo fa, il National Information Assurance Partnership (NIAP) utilizzava il Common Criteria Evaluation & Validation Scheme (CCEVS) per valutare e approvare la sicurezza degli switch KVM.

Il NIAP ha implementato la Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement per l'applicazione dei Common Criteria e non valuta più in base agli Evaluation Assurance Levels (EAL). Questo rafforza le valutazioni concentrandosi sui requisiti di sicurezza specifici della tecnologia.

Di conseguenza, hanno aggiornato il Protection Profile (PP) per gli switch di condivisione delle periferiche a PP 4.0 NIAP Protection Profile for Peripheral Sharing Switch Version 4.0, che sono test relativi al processo di progettazione, test, verifica e spedizione dei prodotti di sicurezza. Questo profilo di protezione è un processo internazionale e standardizzato per la valutazione, la convalida e la certificazione della sicurezza informatica.

Come gli switch KVM sicuri combattono i cyberattacchi

Caratteristiche di sicurezza rigide all'interno degli switch KVM Black Box Secure

- L'isolamento meccanico, elettrico e ottico dei segnali impedisce l'hacking e la fuga di dati -> isolamento assoluto / nessuna fuga di dati tra le porte sicure e il mondo esterno
- Il firmware protetto impedisce ai malintenzionati di riprogrammare o leggere il firmware (ROM non riprogrammabile).
- Le porte USB optoisolate e la cancellazione della cache interna della tastiera mantengono i percorsi dei dati USB isolati elettricamente l'uno dall'altro per evitare perdite di dati USB tra le porte.
- L'emulazione EDID/video e aux sicura limita la rilevazione dei display appena collegati durante le operazioni di commutazione, impedendo la trasmissione di dati indesiderati e non protetti tra i computer e il display.
- Protezione antintrusione dello chassis: dotata di interruttori attivi antimanomissione e di sigilli esterni con ologramma antimanomissione
- Supporto opzionale configurabile Common Access Card (CAC) per smart card, lettori biometrici e registrazione di dispositivi USB esterni.
- Flusso di dati unidirezionale verso periferiche speciali come proiettori, stampanti o sistemi audio.
- Certificato NIAP PP 4.0, il più alto livello di Common Criteria (Protection Profile for Peripheral Sharing Switch Version 4.0).
- Conformi alla normativa TAA e prodotti negli Stati Uniti
- L'ingresso audio è consentito, ma solo se lo switch non supporta altri tipi di periferiche (il microfono non può coesistere con gli altoparlanti).

Testato e certificato secondo l'ultimo profilo di sicurezza NIAP PP 4.0

Gli switch KVM sicuri di Black Box sono progettati per l'uso in applicazioni di difesa e intelligence in cui è necessario proteggere i dati sensibili. Gli switch KVM sicuri di Black Box sono certificati NIAP PP 4.0 e sono dotati delle più elevate caratteristiche di sicurezza che soddisfano gli attuali standard di controllo della sicurezza delle informazioni. Gli switch contengono configurazioni hardware uniche che impediscono la fuga di dati tra i PC e le periferiche collegate, eliminando così qualsiasi potenziale minaccia informatica. NIAP PP 4.0 applica un profilo di protezione di base con moduli individuali per i tipi di periferica.

Sicurezza a più livelli per una rigorosa protezione delle informazioni

L'isolamento assoluto meccanico e dei segnali elettrici e ottici attraverso air gap impedisce la pirateria informatica e la fuga di dati tra le porte e il mondo esterno. Ogni porta dello switch KVM sicuro utilizza i propri canali dati isolati. Switchando su un altro computer, lo switch KVM cancella la cache interna e i dati della tastiera per garantire che non rimangano dati residui nel canale. Il firmware e la ROM sicuri sono bloccati e non sono riprogrammabili, impedendo agli intrusi di leggere, riprogrammare tramite aggiornamenti indesiderati del firmware o rimuovere fisicamente i dati sensibili.

Emulazione di tastiera e mouse

Lo switch KVM sicuro emula la presenza di una tastiera e di un mouse per ogni computer collegato tramite un cavo USB. Sia i computer selezionati che quelli non selezionati mantengono una connessione costante con i controller di emulazione tastiera-mouse dello switch, consentendo una commutazione ultraveloce e limitando il dicovering di periferiche appena collegate durante le operazioni di commutazione. L'emulazione di tastiera e mouse impedisce inoltre la connessione diretta tra le periferiche e i computer collegati, proteggendo i sistemi da potenziali vulnerabilità. Le porte PS/2 sono consentite nella V3.0 e sono vietate nella V4.0.

Protezione antintrusione dello chassis

Gli switch KVM sicuri sono dotati di interruttori attivi antimanomissione, ologramma esterno, sigilli antimanomissione e batteria interna a lunga durata antimanomissione. Se il coperchio viene rimosso dallo chassis, lo switch KVM interrompe la connessione con tutti i PC e le periferiche collegate e disattiva qualsiasi funzionalità per proteggersi da qualsiasi tentativo di intrusione fisica. La risposta alla manomissione è facoltativa nella V4.0 (è obbligatoria nella V3.0), perché alcuni dispositivi possono avere schede intercambiabili per diversi tipi di periferiche (nel qual caso sono sufficienti i sigilli di manomissione). La versione V3.0 vieta la funzionalità audio in (microfono), mentre la versione V4.0 consente l'audio in (ma solo se il dispositivo non supporta altri tipi di periferiche, ad esempio un microfono non può coesistere con gli altoparlanti).

Porta Common Access Card (CAC) completamente configurabile per periferiche USB esterne

Molti switch KVM sicuri supportano dispositivi CAC (Common Access Card), come lettori di smart card e biometrici, rafforzando la sicurezza durante l'utilizzo del dispositivo. Tuttavia, Black Box porta la sicurezza del CAC ancora più in là, consentendo agli amministratori autenticati di registrare e assegnare dispositivi periferici specifici alla porta CAC (opzionale). Gli utenti possono quindi commutare la connessione tra il dispositivo assegnato e la commutazione KVM dei computer collegati.

Limita le connessioni di nuovi monitor durante la commutazione

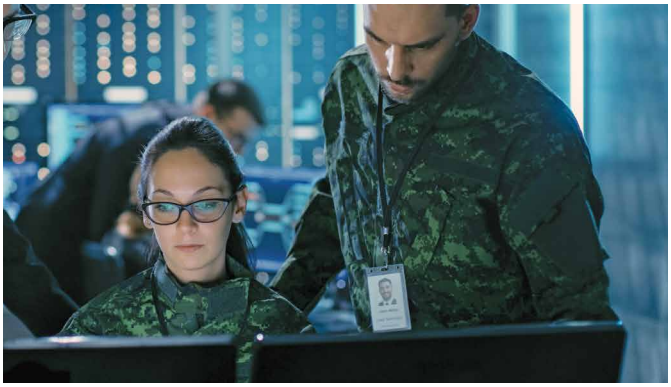
Gli switch KVM sicuri simulano un EDID generico come impostazione predefinita, consentendo il funzionamento della maggior parte dei monitor collegati. I computer selezionati e non selezionati mantengono una connessione costante con i controller di emulazione video e AUX dello switch, consentendo una commutazione ultraveloce e limitando la scoperta di nuovi monitor collegati durante le operazioni di commutazione. Questo protegge i sistemi da potenziali vulnerabilità dovute alla trasmissione di dati indesiderati e non sicuri attraverso le linee DDC. La versione V.4.0 consente l'uso di multiviewer (che però devono utilizzare l'OSD per identificare il canale video attivo).

Casi d'uso

Ideale per più settori

- Governo
- Difesa e militare
- Sale di controllo per la gestione del traffico
- Banche e finanza
- Formazione scolastica
- Assistenza sanitaria
- Dipartimenti di R&S
- Utilità

Casi d'uso

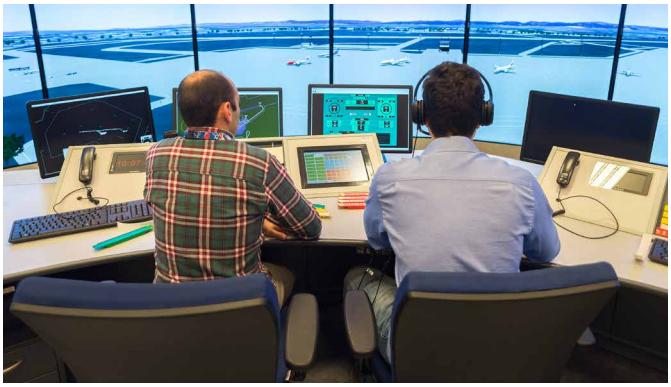


Centro comunicazioni della Difesa

Un cliente del settore della difesa si è rivolto a Black Box con due problemi urgenti: un accesso alla rete inefficiente e uno spazio di lavoro disordinato.

I loro operatori dovevano accedere a più reti informatiche in centri di comunicazione sicuri. Si trattava di un processo che richiedeva molto tempo perché ogni rete di computer richiedeva una tastiera, un monitor e un mouse separati, il che significava che l'operatore doveva spostarsi tra i diversi sistemi per accedere ai dati sensibili e alle reti di intelligence. Questo richiedeva anche un tavolo per tutti e sei i diversi monitor, le sei diverse tastiere e i sei diversi mouse, il che rendeva lo spazio di lavoro disordinato e angusto.

Per superare queste sfide, hanno acquistato uno switch KVM sicuro a 8 porte di Black Box che ha ridotto la configurazione a un solo monitor, una sola tastiera e un solo mouse, facendo risparmiare tempo prezioso agli operatori che dovevano passare da una rete all'altra e liberando molto spazio su scrivanie e uffici. Ora operano in modo più efficiente in uno spazio di lavoro pulito, garantendo al contempo che i loro dati vitali non vengano compromessi.



Polizia

Un'azienda ha contattato Black Box quando ha richiesto una soluzione altamente sicura per un progetto di polizia. Gli ingegneri del progetto dovevano passare da una rete aperta (verde) a una sicura (rossa). Black Box ha suggerito lo Switch KVM sicuro DVI USB a 4 porte, che soddisfa perfettamente tutte le loro esigenze. Sono già stati installati oltre 1.000 switch KVM sicuri.

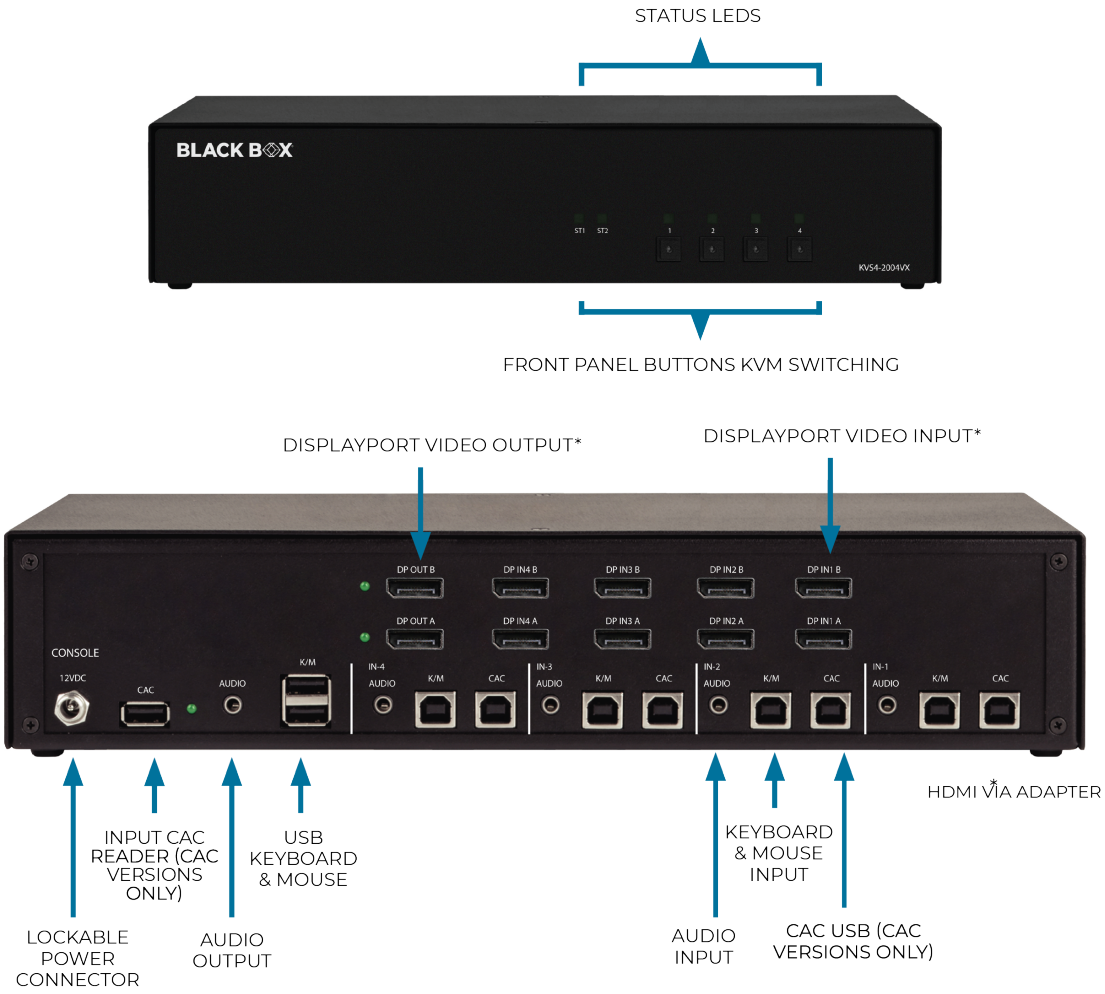
Impresa

La condivisione di risorse globali e la necessità di collaborare in tempo reale hanno portato a una crescente rete di dati. Se da un lato l'interconnessione aiuta le organizzazioni a lavorare insieme in modo più efficiente ed efficace, dall'altro le rende sempre più vulnerabili a devastanti attacchi informatici. In definitiva, i sistemi che accedono a Internet devono essere tenuti lontani da altri sistemi utilizzati per dati aziendali o personali sensibili. Per mantenere la sicurezza delle informazioni, molte organizzazioni stanno sostituendo gli switch KVM standard con switch KVM sicuri.

Panoramica del prodotto Secure KVM

Design sicuro dello switch KVM

Esempio di switch KVM sicuro a 4 porte, utente singolo, DisplayPort, USB e CAC KVS4-2004VX



Tipi di switch KVM desktop sicuri certificati NIAP 4.0

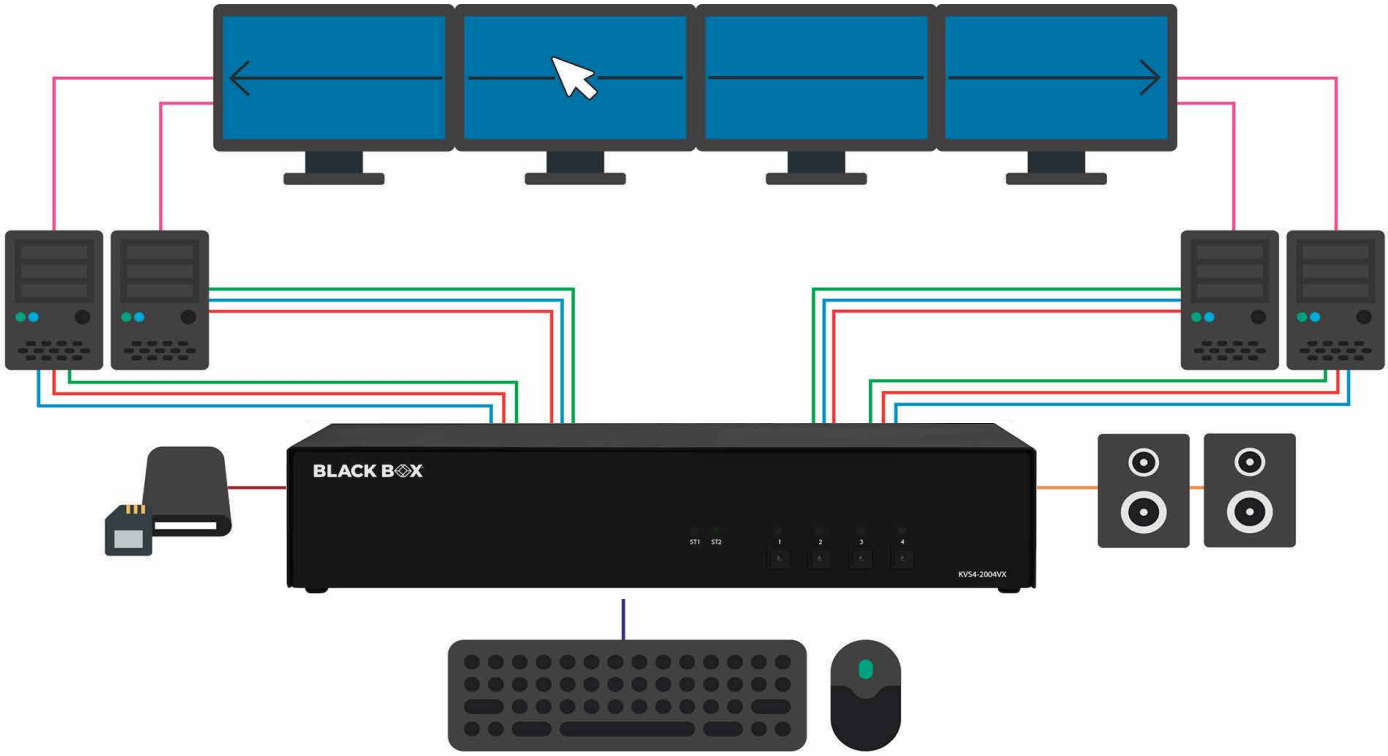
Switch KVM desktop sicuri, utente singolo

- Condividete una singola console utente tra due, quattro o otto computer.
- Disponibile con video DVI-I, DisplayPort o HDMI/ DisplayPort
- Video di alta qualità DisplayPort 1.2/HDMI con risoluzioni fino a 4K@60Hz e la migliore risoluzione DVI-I dual-link fino a 2560x1600 @ 60Hz
- Scegliete tra i modelli con connessioni alla console a uno, due o quattro monitor.
- Tastiera/mouse USB e audio stereo
- Disponibile con o senza supporto CAC
- Prodotto, testato e certificato negli USA

Trovate il prodotto giusto nel selettore a pagina 9 e 10.

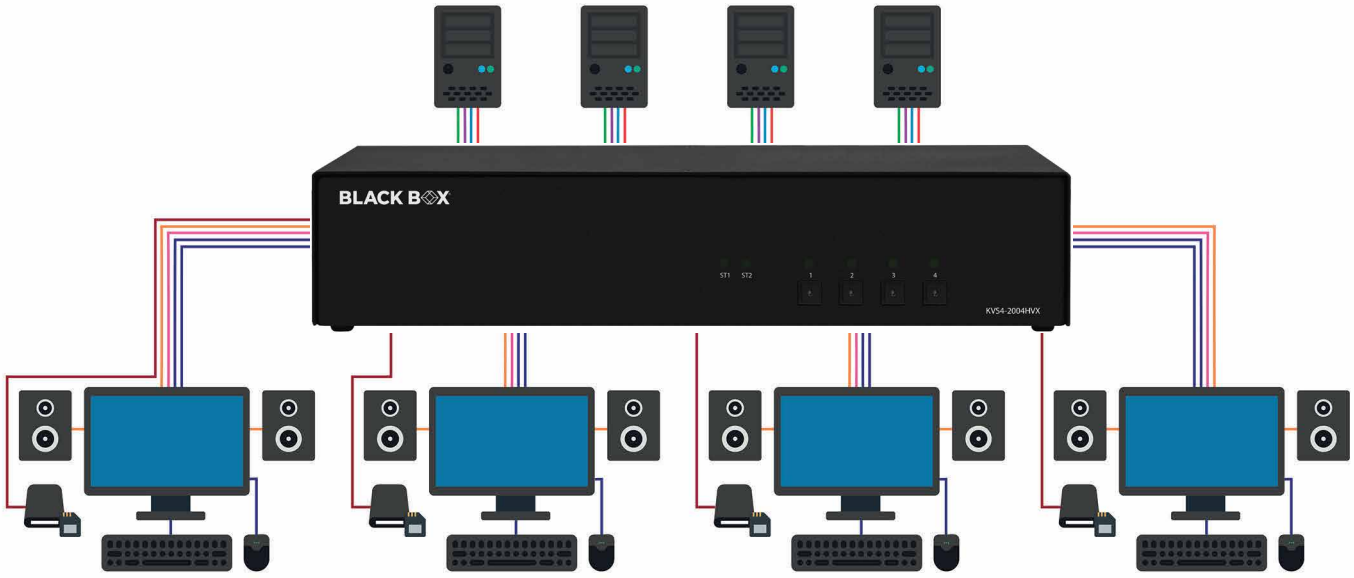
Switch KM sicuri certificati NIAP 4.0

- Passare da un monitor all'altro con il mouse (Glide & Switch)
- Visualizzazione simultanea di più fonti attraverso connessioni dedicate a computer/monitor
- Supporto audio stereo
- Condividete un'unica console utente con tastiera e mouse USB tra quattro o otto computer.
- Supporto audio stereo
- Disponibile con o senza supporto CAC
- Prodotto, testato e certificato negli USA



Switch KVM sicuro certificato NIAP 4.0 - FlexPort HDMI/Porta display

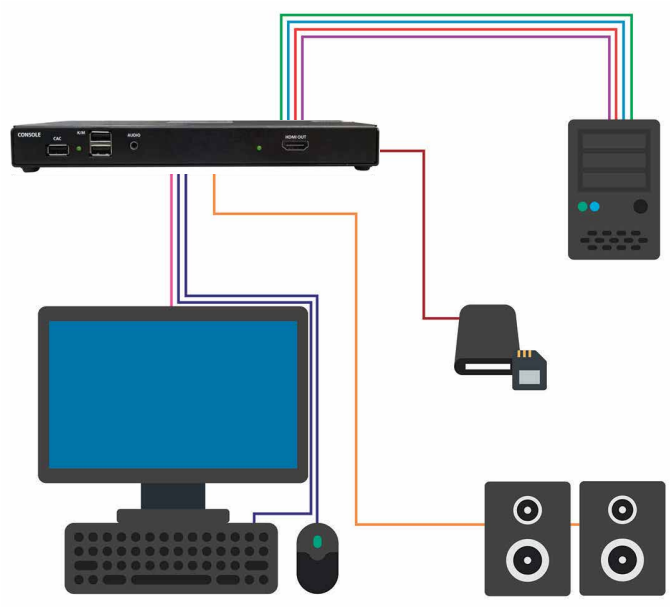
- Funzionamento sicuro di tastiera, video e mouse su un massimo di due o quattro computer con uno o due monitor HDMI/DisplayPort grazie alla tecnologia FlexPort.
- Certificato per il profilo di protezione NIAP per dispositivi di condivisione di periferiche versione 4.0
- Supporta risoluzioni fino a 4K@60Hz
- Prodotto, testato e certificato negli Stati Uniti
- Alimentazione esterna



Trovate il prodotto giusto nel selettore a pagina 9 e 10.

Difensore sicuro delle periferiche KVM, certificato NIAP 4.0 - CAC

- Isola un computer dal monitor DVI-I, HDMI o DisplayPort, dalla tastiera, dal mouse e dal CAC per garantire sicurezza e protezione.
- Certificato per il profilo di protezione NIAP per dispositivi di condivisione di periferiche versione 4.0
- Interfaccia video a monitor singolo
- Protegge le periferiche non protette
- Testato e certificato secondo lo schema USA
- Alimentazione esterna
- Assicura un flusso di dati unidirezionale di video, USB e audio dal computer alla periferica.
- Supporta la maggior parte dei monitor attraverso l'apprendimento/emulazione EDID sicura
- Ideale per le sale conferenze, per proteggere i computer portatili da intrusioni attraverso la connessione condivisa del display.



Trovate il prodotto giusto nel selettore a pagina 9 e 10.

SOLUZIONI DI PRODOTTO NIAP 4.0

SWITCH KVM SICURO, CERTIFICATO NIAP 4.0, DISPLAYPORT					
					
ARTICOLO #	KVS4-1004V	KVS4-2002V	KVS4-2004V	KVS4-2004VX	KVS4-2008VX
Descrizione	2 porte, monitor singolo, DisplayPort	2 porte, doppio monitor, DisplayPort	4 porte, doppio monitor, DisplayPort	4 porte, doppio monitor, DisplayPort, CAC	8 porte, doppio monitor, DisplayPort, CAC
Numero di fonti	2	2	4	4	8
Compatibilità con il computer	Windows®, Mac®, e Linux® OS				
Max. Risoluzione	Fino a 4K@60Hz				
Compatibilità del monitor	La maggior parte dei monitor grazie all'apprendimento e all'emulazione EDID sicura				
PORTE ALLA CONSOLE UTENTE					
Connessione/i del monitor	(1) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort
Connessioni tastiera/mouse	(2) USB 2.0 tipo A, solo tastiera e mouse				
Uscita audio	(1) Jack audio da 3,5 mm con uscite altoparlanti bilanciate e commutazione				
Supporto CAC	NO	NO	NO	(1) USB tipo A, completamente configurabile	(1) USB tipo A, completamente configurabile
PORTE AI COMPUTER					
Connessione/i del monitor	(1) DisplayPort per sorgente	(2) DisplayPort per sorgente	(2) DisplayPort per sorgente	(2) DisplayPort per sorgente	(2) DisplayPort per sorgente
Connessioni tastiera/mouse	(1) USB 2.0 Tipo B con emulazione USB per sorgente				
Uscita audio	(1) Jack audio da 3,5 mm per sorgente				
Supporto CAC	NO	NO	NO	(1) USB tipo B per sorgente	(1) USB tipo B per sorgente

SWITCH KVM SICURO, CERTIFICATO NIAP 4.0, DVI-D					
					
ARTICOLO #	KVS4-1002D	KVS4-1004D	KVS4-2002D	KVS4-2004D	KVS4-2008D
Descrizione	4 porte, monitor singolo, DVI-D	4 porte, monitor singolo, DVI-D	2 porte, doppio monitor, DVI-D	4 porte, doppio monitor, DVI-D	8 porte, doppio monitor, DVI-D
Numero di fonti	4	4	2	4	8
Compatibilità con il computer	Windows®, Mac®, e Linux® OS				
Max. Risoluzione	2560 x 1600 a 60 Hz				
Compatibilità del monitor	La maggior parte dei monitor attraverso l'apprendimento e l'emulazione EDID sicura				
PORTE ALLA CONSOLE UTENTE					
Connessione/i del monitor	(1) DVI-D	(1) DVI-D	(2) DVI-D	(2) DVI-D	(2) DVI-D
Connessioni tastiera/mouse	(2) USB 2.0 tipo A, solo tastiera e mouse				
Uscita audio	(1) Jack audio da 3,5 mm con uscite altoparlanti bilanciate e commutazione				
Supporto CAC	NO	NO	NO	NO	NO
PORTE AI COMPUTER					
Ingresso/i video	(1) DVI-D per sorgente	(1) DVI-D per sorgente	(2) DVI-D per sorgente	(2) DVI-D per sorgente	(2) DVI-D per sorgente
Ingressi da tastiera/mouse	(1) USB 2.0 tipo B con emulazione USB per sorgente				
Uscita audio	(1) Jack audio da 3,5 mm per sorgente				
Supporto CAC	NO	NO	NO	NO	NO

SWITCH KVM SICURO, CERTIFICATO NIAP 4.0, FLEXPORT HDMI/PORTA DISPLAY				
				
Articolo #	KVS4-1004HV	KVS4-2002HV	KVS4-2004HV	KVS4-2004HVX
Descrizione	4 porte, monitor singolo, FlexPort HDMI/Porta display	2 porte, doppio monitor, FlexPort HDMI/Porta display	4 porte, doppio monitor, FlexPort HDMI/Porta display	4 porte, doppio monitor, FlexPort HDMI/Porta display, CAC
Numero di fonti	4	2	4	4
Compatibilità con il computer	Windows®, Mac®, e Linux® OS			
Max. Risoluzione	Fino a 4K@60Hz			
Compatibilità del monitor	La maggior parte dei monitor grazie all'apprendimento e all'emulazione EDID sicura			
PORTE ALLA CONSOLE UTENTE				
Connessione/i del monitor	(1) FlexPort HDMI/DisplayPort	(2) FlexPort HDMI/ DisplayPort	(2) FlexPort HDMI/ DisplayPort	(2) FlexPort HDMI/DisplayPort
Connessioni tastiera/mouse	(2) USB 2.0 tipo A, solo tastiera e mouse			
Uscita audio	(1) Jack audio da 3,5 mm con uscite altoparlanti bilanciate e commutazione			
Supporto CAC	NO	NO	NO	(1) USB tipo A, completamente configurabile
PORTE AI COMPUTER				
Ingresso/i video	(1) FlexPort HDMI/DisplayPort per sorgente	(2) FlexPort HDMI/ DisplayPort per sorgente	(2) FlexPort HDMI/ DisplayPort per sorgente	(2) FlexPort HDMI/DisplayPort per sorgente
Ingressi da tastiera/mouse	(1) USB 2.0 tipo B con emulazione USB per sorgente			
Uscita audio	(1) Jack audio da 3,5 mm per sorgente			
Supporto CAC	NO	NO	NO	(1) USB tipo B per sorgente

DIFENSORE SICURO DELLE PERIFERICHE KVM, CERTIFICATO NIAP 4.0 - CAC			
			
Articolo #	KVS4-8001DX	KVS4-8001HX	KVS4-8001VX
Descrizione	DVI-D, CAC	HDMI, CAC	DisplayPort, CAC
Compatibilità con il computer	Windows®, Mac®, e Linux® OS		
Max. Risoluzione	2560 x 1600 @ 60Hz (DVI-D) Fino a 4K@60Hz (modelli HDMI e DisplayPort)		
Compatibilità del monitor	La maggior parte dei monitor grazie all'apprendimento e all'emulazione EDID sicura		
PORTE ALLA CONSOLE UTENTE			
Connessione/i del monitor	(1) DVI-D a 23 pin (femmina)	(1) HDMI 1.4	(1) DisplayPort
Connessioni tastiera/mouse	(2) USB Tipo-A solo per il collegamento di tastiera e mouse (1) USB Tipo-A per il collegamento al CAC	(2) USB Tipo-A solo per il collegamento di tastiera e mouse (1) USB Tipo-A per il collegamento al CAC	(2) USB Tipo-A solo per il collegamento di tastiera e mouse (1) USB Tipo-A per il collegamento al CAC
Uscita audio	(1) Connettore stereo 3,5 mm femmina	(1) Connettore stereo 3,5 mm femmina	(1) Connettore stereo 3,5 mm femmina
Supporto CAC	(1) USB tipo A, completamente configurabile	(1) USB tipo A, completamente configurabile	(1) USB tipo A, completamente configurabile
PORTE AI COMPUTER			
Ingresso video	(1) DVI-D a 23 pin (femmina)	(1) HDMI 1.4	(1) DisplayPort
Ingressi da tastiera/mouse	(1) USB Tipo-B	(1) USB Tipo-B	(1) USB Tipo-B
Uscita audio	(1) Connettore stereo 3,5 mm femmina	(1) Connettore stereo 3,5 mm femmina	(1) Connettore stereo 3,5 mm femmina
Supporto CAC	(1) USB tipo B	(1) USB tipo B	(1) USB tipo B

BLACK BOX®

Perché Black Box?

Competenza

Gli ingegneri di progetto Black Box possono assistere nella valutazione, nella progettazione, nell'implementazione e nella formazione del sistema.

Ampiezza

Black Box offre la suite più completa di soluzioni KVM ingegnerizzate del settore.

Supporto

A dimostrazione del nostro impegno per la completa soddisfazione, il nostro team dedicato e altamente qualificato di supporto tecnico è disponibile telefonicamente gratuitamente tutti i giorni dell'anno.

Garanzie

Gli switch KVM Secure hanno una garanzia di 3 anni e sono disponibili opzioni di estensione.

Esperienza

Fornendo soluzioni tecnologiche all'avanguardia dal 1976, Black Box aiuta più di 175.000 clienti in 150 paesi a creare, gestire, ottimizzare e proteggere le infrastrutture IT.

Center of Excellence

Black Box offre un centro di eccellenza con servizi professionali e contratti di assistenza che aiutano a ottimizzare i sistemi dei clienti e a massimizzare i tempi di attività.

Service Level Agreements

I nostri Service Level Agreement consentono ai clienti di accedere a supporto tecnico, formazione sui prodotti, ingegneri applicativi dedicati e altro ancora.

SCOPRI DI PIÙ BLACKBOX.COM/SECUREKVM