

# SWITCH KVM SICURI

BROCHURE SULLE SOLUZIONI





## CONTRASTA LE INNUMEREVOLI MINACCE PER LA SICUREZZA CHE INSORGONO QUANDO SI CONDIVIDONO PERIFERICHE TRA RETI INFORMATICHE CON DIVERSI LIVELLI DI SICUREZZA

### PERCHÉ SCEGLIERE SWITCH KVM SICURI

Le cyber-minacce sono in continua evoluzione e diventano ogni giorno sempre più frequenti e più sofisticate. La scelta di affidarsi alla tecnologia, la condivisione di risorse globali e la necessità di una collaborazione in tempo reale hanno portato ad una rete di dati in crescita. Sebbene l'interconnettività ci aiuti a lavorare insieme in modo più efficace ed efficiente, ci rende tuttavia sempre più vulnerabili a devastanti attacchi informatici.

Le più importanti agenzie per la difesa e altri organizzazioni simili utilizzano misure di sicurezza avanzate per isolare le reti e tutelare le informazioni da minacce esterne. Esiste tuttavia un luogo in cui convivono reti isolate e informazioni sensibili: il desktop dell'utente.

Gli switch KVM non sicuri sono suscettibili ad attacchi informatici con il rischio che cyber criminali riescano ad accedere a dati classificati. Se un cyber criminale decide di rubare informazioni da un server classificato, può semplicemente collegare una chiavetta USB contenente il malware di un virus ad uno switch KVM e accedere così a più server anziché a uno solo. Gli switch KVM sono inoltre suscettibili ad un utilizzo doloso di monitor LCD (tramite un segnale EDID), di microfoni o di un'inadeguata implementazione CAC.

I cyber criminali inoltre sono in grado di ricavare informazioni sull'hardware per mezzo di onde sonore emesse dagli switch KVM non sicuri. Sono in grado di ottenere sequenze ROM programmabili da onde sonore, il che consente ai cyber criminali di riconfigurare o riprogrammare il server per renderlo non sicuro. Con questi metodi tantissime informazioni classificate rischiano di finire nelle mani sbagliate e di essere utilizzate per danneggiare l'organizzazione.

### SWITCH KVM TRADIZIONALI

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

La tecnologia KVM offre soluzioni di monitoraggio per automazione, processi e flussi di lavoro. Garantisce agli utenti una migliore operabilità e un rapido ritorno sull'investimento grazie alla migliore ergonomia dello spazio di lavoro e della migliore produttività. Gli switch KVM consentono agli utenti di risparmiare spazio riducendo i dispositivi di interfaccia, di abbattere i costi eliminando periferiche ridondanti e di reagire con maggiore rapidità in situazioni critiche.





SS4P-DH-DP-UCAC



## GLI SWITCH KVM SICURI PROTEGGONO I DATI SENSIBILI CLASSIFICATI

Uno switch KVM sicuro è uno switch per desktop a 2, 4, 8 o 16 porte che garantisce il controllo e la separazione di PC collegati alle reti con diverse classificazioni di sicurezza. Al contrario degli switch KVM tradizionali, gli switch KVM sicuri possono essere controllati esclusivamente utilizzando un comando a pulsante. I comandi mediante scelte rapide sono disabilitati, a garanzia di un accesso consentito esclusivamente agli utenti giusti.

Gli KVM sicuri non permettono ad una chiavetta USB che non viene riconosciuta di accedere a nessun tipo di informazione: consentono infatti agli amministratori di scegliere quali dispositivi USB autorizzare e riconoscere. Questi switch sono caratterizzati da ROM non riprogrammabile che impedisce il recupero di informazioni hardware dalle onde sonore. Ma tutto questo è solo la punta dell'iceberg. Gli switch KVM sicuri fanno molto, molto più che proteggere le agenzie governative dalle più terrificanti cyber minacce odierne.

Ora, dal momento che la sicurezza desktop diventa sempre più critica, Black Box ha deciso di presentare una propria linea di switch KVM e KM sicuri. Gli switch KVM sicuri con certificazione NIAP 3.0 garantiscono il totale isolamento tra reti di computer pur condividendo la stessa serie di periferiche. Ciascuna porta utilizza il proprio canale dati isolato, il che garantisce l'assoluta impossibilità di perdere dei dati tra le porte in caso di informazioni classificate e porte non attendibili. Un'ampia gamma di funzioni di sicurezza li protegge contro cyber-minacce mentre il design antimanomissione dell'hardware ne impedisce la manipolazione fisica.

### PROFILO DI PROTEZIONE NIAP PER SWITCH KVM SICURI

Fino a poco tempo fa la NIAP (National Information Assurance Partnership) si avvaleva del CCEVS (Common Criteria Evaluation & Validation Scheme) per valutare e approvare gli switch KVM ai fini della sicurezza.

La NIAP ha istituito un comitato di gestione CCRA (Common Criteria Recognition Arrangement) per l'applicazione dei criteri comuni e non valuta più a fronte dei livelli di garanzia della valutazione (Evaluation Assurance Levels - EAL). Lo scopo è rafforzare le

valutazioni concentrandosi su requisiti di sicurezza specifici per la tecnologia.

Di conseguenza è stato aggiornato il profilo di protezione (PP) degli switch di condivisione periferica a Profilo di protezione NIAP 3.0 PPS per switch a condivisione periferica versione 3.0, che comprende test relativi al processo di progettazione, collaudo, verifica e spedizione di prodotti per la sicurezza. Questo profilo di sicurezza è un processo standardizzato internazionale di certificazione, convalida e valutazione della sicurezza delle tecnologie di informazione.

### RIGIDE FUNZIONI DI SICUREZZA ALL'INTERNO DEGLI SWITCH KVM SICURI DI BLACK BOX

- Isolamento meccanico, elettrico e ottico dei segnali al fine di prevenire l'hackeraggio e la perdita di dati -> isolamento assoluto / nessuna perdita di dati tra le porte sicure e il mondo esterno
- Il firmware protetto impedisce a eventuali intrusi di riprogrammare o di leggere il firmware (ROM non riprogrammabile)
- Le porte USB opto-isolate e la pulizia della cache interna/tastiera tengono il percorso dati USB isolato elettricamente le une dalle altre onde evitare la perdita di dati USB tra le porte
- L'emulazione EDID/video e aux sicura restringe la scoperta di display appena collegati durante le operazioni di switching. In questo modo si impedisce la trasmissione di dati indesiderati e non sicuri tra i computer e il display
- Protezione antintrusione dello chassis: grazie a switch antimanomissione attivi e a sigilli olografici esterni in grado di rivelare eventuali tentativi di manomissione
- Supporto CAC (Common Access Card - Scheda di accesso comune) configurabile opzionale per smart card, lettori biometrici e registrazione di dispositivi USB esterni
- Flusso di dati unidirezionale verso speciali periferiche quali un proiettore, una stampante o un impianto audio
- Certificazione conforme a NIAP PP 3.0, il livello più alto tra i criteri comuni (Profilo di protezione per switch di condivisione periferica versione 3.0)
- Conformità con TAA e made in U.S

---

#### TESTATI E CERTIFICATI SULLA BASE DEL PIÙ RECENTE PROFILO DI SICUREZZA NIAP PP 3.0

Gli switch KVM sicuri di Black Box sono progettati per essere utilizzati in applicazioni sicure di difesa ed intelligence dove è necessario proteggere i dati sensibili. Gli switch KVM sicuri di Black Box sono certificati NIAP PP 3.0 e dotati di funzioni di sicurezza all'avanguardia che soddisfano gli odierni standard di controllo sulla protezione delle informazioni. Gli switch contengono configurazioni hardware uniche che impediscono la perdita di dati tra i PC e le periferiche collegate eliminando così il potenziale rischio di cyber minaccia.

#### SICUREZZA MULTILIVELLO PER UNA RIGOROSA TUTELA DELLE INFORMAZIONI

Un isolamento assoluto dei segnali meccanici, elettrici e ottici mediante l'air gap previene il rischio di hacking e di perdita dei dati tra le porte e il mondo esterno. Ciascuna porta dello switch KVM sicuro utilizza i propri canali dati isolati. Mediante lo switching anticipato su un altro computer target, lo switch KVM cancella la cache interna e i dati da tastiera per far sì che nel canale non rimangano dati residui. Il firmware e il ROM sicuro fisso non sono riprogrammabili e impediscono agli intrusi la lettura, la riprogrammazione per mezzo di aggiornamenti firmware indesiderati o la rimozione fisica.

#### PROTEZIONE ANTINTRUSIONE DELLO CHASSIS

Gli switch KVM sicuri sono dotati di switch antimanomissione attivi; sigilli olografici esterni in grado di rivelare eventuali tentativi di manomissione e una batteria interna antimanomissione di lunga durata. In caso di rimozione del coperchio dallo chassis, lo switch KVM disattiva la connessione con tutti i PC e le periferiche collegate e ne disabilita qualsiasi funzionalità così da proteggerli contro qualsiasi eventuale tentativo di intrusione fisica.

#### EMULAZIONE DI TASTIERA E MOUSE

Lo switch KVM sicuro emula la presenza di una tastiera e di un mouse per ciascun computer collegato per mezzo di un cavo USB. Sia i computer selezionati che quelli non selezionati mantengono una connessione costante con i controller di emulazione tastiera e mouse dello switch, garantendo così uno switching ultra-rapido e restringendo la scoperta di periferiche appena collegate durante le operazioni di switching. L'emulazione di tastiera e mouse impedisce inoltre la connessione diretta tra le periferiche e i computer collegati, schermando i sistemi contro potenziali vulnerabilità.

#### PORTA CAC (COMMON ACCESS CARD - SCHEDA DI ACCESSO COMUNE) INTERAMENTE PROGRAMMABILE PER PERIFERICHE USB ESTERNE

Molti switch KVM sicuri supportano dispositivi CAC (Common Access Card - Scheda di accesso comune) quali lettori di smart card e biometrici che rafforzano la sicurezza mentre il dispositivo è in uso. Tuttavia Black Box prende la sicurezza CAC ancora più seriamente, consentendo agli amministratori autenticati di registrare e assegnare specifici dispositivi periferici alla porta CAC (optional). Gli utenti possono quindi attivare la connessione tra il dispositivo assegnato unitamente allo switching KVM dei computer collegati.

#### LIMITAZIONE DI NUOVE CONNESSIONI MONITOR DURANTE LO SWITCHING

Gli switch KVM sicuri simulano di default un EDID generico consentendo quindi di far funzionare la maggior parte dei monitor collegati. Sia i computer selezionati che quelli non selezionati mantengono una connessione costante con i controller di emulazione video e AUX dello switch, garantendo così uno switching ultra-rapido e restringendo la scoperta di monitor appena collegati durante le operazioni di switching. I sistemi sono così schermati contro potenziali vulnerabilità imputabili ad una trasmissione di dati indesiderati e non sicuri tramite le linee DDC.



**SOLUZIONE IDEALE PER SVARIATI SETTORI**



GOVERNO



SETTORE MILITARE  
E DELLA DIFESA



CONTROL ROOM PER LA  
GESTIONE DEL TRAFFICO



SETTORE BANCARIO  
E FINANZIARIO



ISTRUZIONE



SANITÀ



REPARTI R&D

**CASI D'USO**



**CENTRO COMUNICAZIONI DELLA DIFESA**

Un cliente della difesa si presentò da Black Box con due problemi spinosi: un accesso inefficiente alla rete e uno spazio di lavoro disordinato.

Gli operatori dovevano poter accedere a più reti informatiche in centri comunicazioni sicuri. Si trattava di un processo dispendioso in termini di tempo poiché ciascuna rete richiedeva una tastiera, un monitor e un mouse a parte, il che significava che l'operatore era tenuto a spostarsi tra diversi sistemi per poter accedere a dati sensibili e a reti intelligenti. A tutto ciò bisognava aggiungere la necessità di un tavolo adatto ad alloggiare sei diversi monitor, sei diverse tastiere e sei diversi mouse, con il risultato di ottenere uno spazio di lavoro disordinato e limitato.

Per ovviare a tutte queste sfide l'azienda ha acquistato uno switch KVM sicuro a 8 porte di Black Box che ha consentito loro di ridurre la configurazione ad un solo monitor, una sola tastiera e un solo mouse. Per gli operatori costretti a passare da una rete all'altra tutto ciò si è tradotto in un risparmio di tempo prezioso e nel recupero di tantissimo spazio sul tavolo e nell'ufficio. Ora possono lavorare in modo più efficiente in uno spazio di lavoro pulito senza nessun rischio che i dati di vitale importanza rischino di essere in alcun modo compromessi.



**SETTORE AEROSPAZIALE**

Una società ha contattato Black Box perché alla ricerca di una soluzione ad alta sicurezza per un progetto aerospaziale. I project engineer dovevano scegliere tra una rete aperta (verde) e una sicura (rossa). Black Box ha suggerito loro l'impiego di uno switch KVM sicuro USB DVI a 4 porte che si adatta perfettamente a tutte le loro esigenze. Sono già stati installati più di 1.000 switch KVM sicuri.

**SETTORE AZIENDALE**

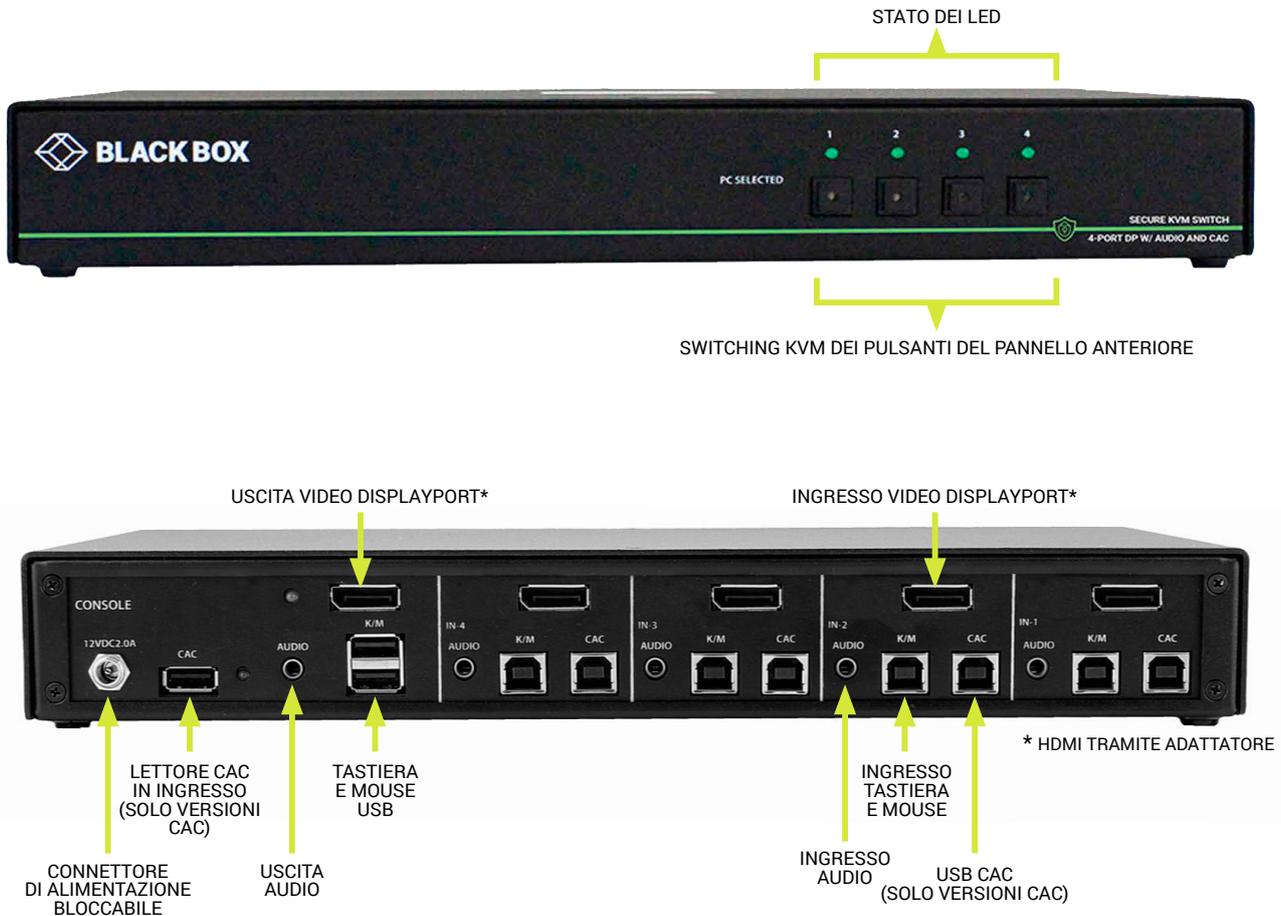
La condivisione di risorse globali e la necessità di una collaborazione in tempo reale hanno portato ad una rete di dati in crescita. Sebbene l'interconnettività aiuti le organizzazioni a lavorare insieme in modo più efficace ed efficiente, le rende tuttavia sempre più vulnerabili a devastanti attacchi informatici. In definitiva i sistemi che accedono a Internet devono poter essere isolato da altri sistemi che vengono utilizzati per dati sensibili o personali. Per garantire la protezione delle proprie informazioni, molte organizzazioni stanno iniziando a sostituire gli switch standard con switch KVM sicuri.



# PANORAMICA DEI PRODOTTI KVM SICURI

## DESIGN DI UNO SWITCH KVM SICURO

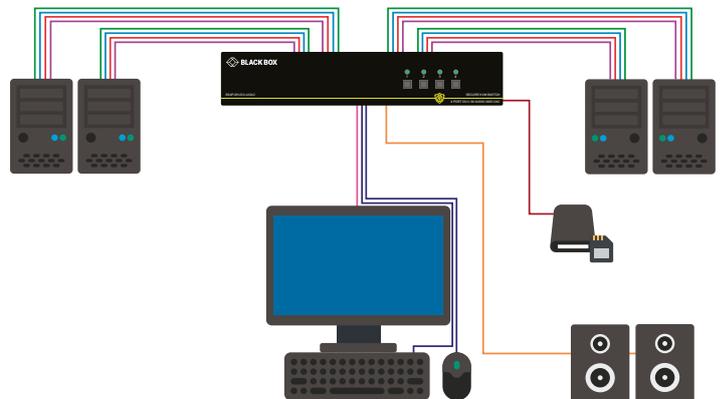
Esempio di switch KVM sicuro a 4 porte, utente singolo, Displayport, USB e CAC (SS4P-SH-DP-UCAC)



## TIPI DI SWITCH KVM PER DESKTOP SICURI

### SWITCH KVM PER DESKTOP SICURI, UTENTE SINGOLO

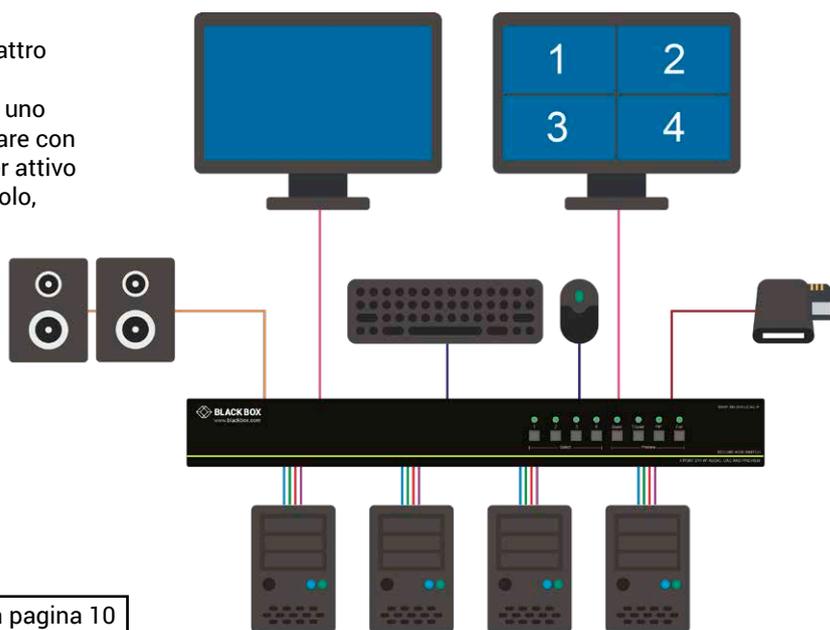
- Condivisione di una singola console utente tra due, quattro, otto o 16 computer
- Disponibili con DVI-I, DisplayPort o video HDMI
- Video DisplayPort 1.2/HDMI di alta qualità con risoluzioni fino a 4K Ultra-HD (3840×2160 a 30Hz) e ottima risoluzione DVI-I a doppio collegamento fino a 2560 x1600 a 60Hz
- Possibilità di scelta tra modelli con connessioni a monitor singolo, doppio o quadruplo alla console
- Tastiera/mouse USB più stereo audio
- Disponibili con o senza supporto CAC
- Certificazione NIAP 3.0



**i** Trova il prodotto giusto per te utilizzando il selettore alle pagine 9 e 10

## SWITCH KVM SICURO DVI-I, UTENTE SINGOLO CON DISPLAY A FINESTRE 4-IN-1

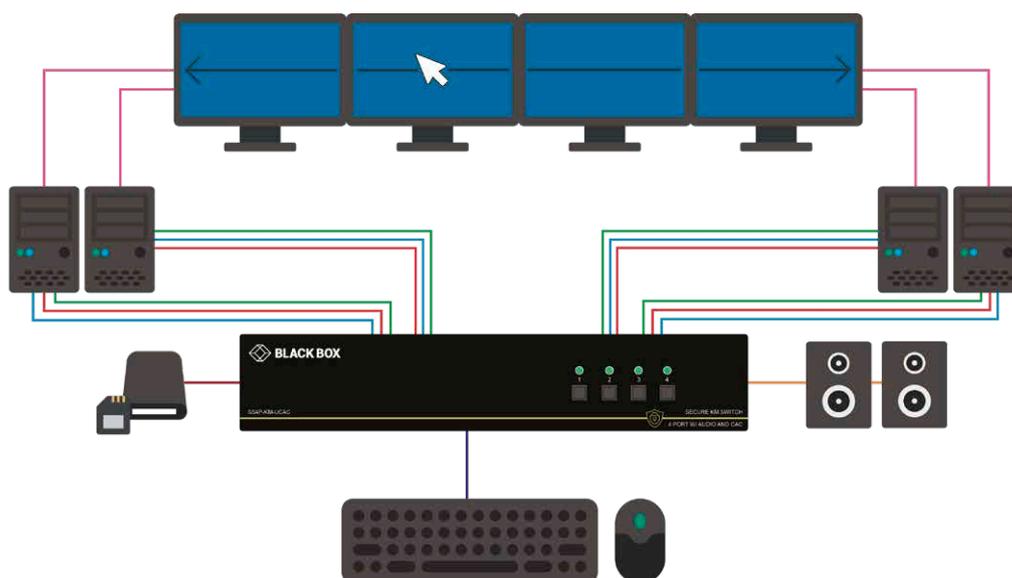
- Condivisione di una singola console utente tra quattro computer
- Monitoraggio concomitante di tutte le sorgenti su uno schermo suddiviso 4-in-1 pur continuando a lavorare con un secondo display a schermo intero sul computer attivo
- Video DVI-I che supporta DVI a collegamento singolo, DVI a collegamento doppio e VGA
- Migliore risoluzione a doppio collegamento fino a 2560 x1600
- Tastiera/mouse USB più stereo audio
- Supporto CAC per lettori di smart card e assegnazione di speciali periferiche
- La certificazione NIAP 3.0 non prevede un profilo di verifica per i display a finestre.



**i** Trova il prodotto giusto utilizzando il selettore a pagina 10

## SWITCH KM PER DESKTOP SICURI

- Commutazione consentita mediante spostamento del mouse da un monitor all'altro (Glide & Switch)
- Visualizzazione concomitante di più sorgenti mediante connessioni computer/monitor dedicate
- Supporto audio stereo
- Condivisione di un'unica console utente con tastiera e mouse USB tra quattro oppure otto computer
- Supporto audio stereo
- Disponibili con o senza supporto CAC
- Certificazione NIAP 3.0



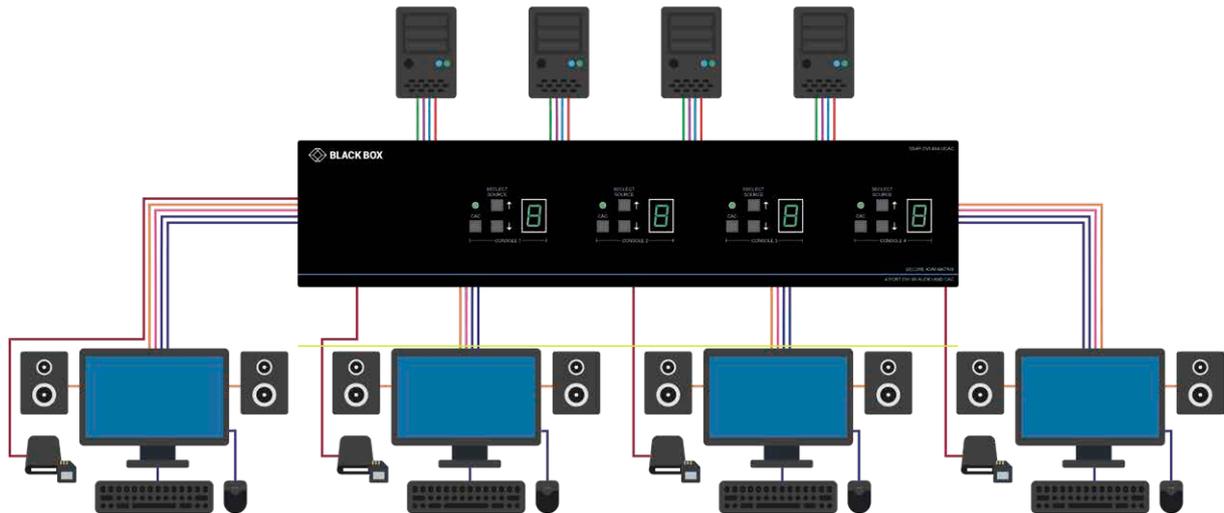
**i** Trova il prodotto giusto utilizzando il selettore a pagina 11

## PANORAMICA DEI PRODOTTI KVM SICURI

### SWITCH A MATRICE KVM SICURI DVI-I, MULTIUTENTE

- Accesso per due o quattro utenti a quattro oppure otto computer
- Video DVI-I che supporta DVI a collegamento singolo, DVI a collegamento doppio e VGA fino a 2560 x1600
- Tastiera/mouse USB più stereo audio
- Supporto CAC per lettori di smart card e assegnazione di speciali periferiche

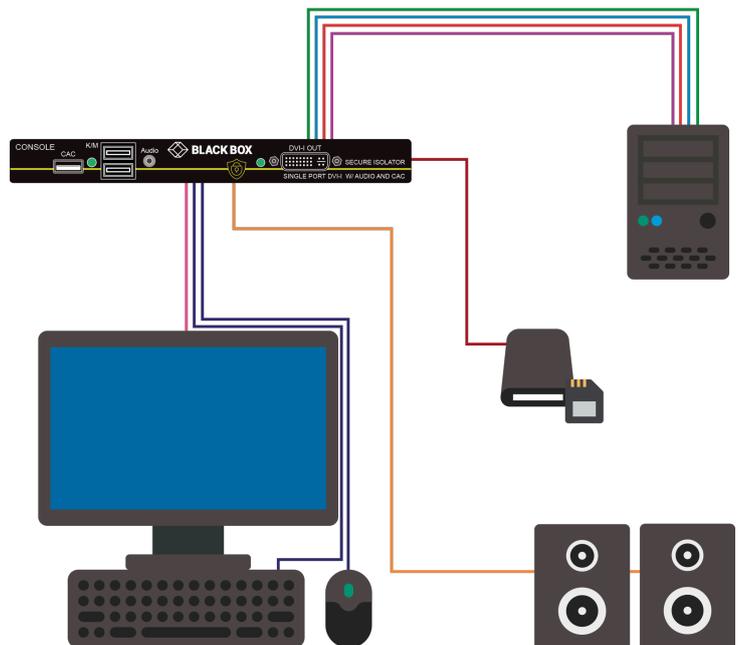
- Supporto del maggior numero di monitor mediante emulazione/EDID learning sicuri
- Compatibili con Windows, Mac e Linux OS
- Certificazione NIAP 3.0



**i** Trova il prodotto giusto utilizzando il selettore a pagina 11

### DISPOSITIVO DI PROTEZIONE PERIFERICHE SICURO

- Blocca la connessione diretta tra un PC host o un laptop e un dispositivo periferico esposto a minacce per la sicurezza come una stampante, un proiettore, un altoparlante o qualsiasi altro dispositivo periferico che condivide l'accesso con una computer o una rete classificati
- Garanzia di un flusso di dati unidirezionale di video, USB e audio dal computer alla periferica
- Supporto di video DVI-I, USB e audio
- Supporto del maggior numero di monitor mediante emulazione/EDID learning sicuri
- Supporto audio stereo
- Compatibili con Windows, Mac e Linux OS
- Supporto CAC
- Certificazione NIAP 3.0



**i** Trova il prodotto giusto utilizzando il selettore a pagina 10

**SWITCH KVM DISPLAYPORT SICURI CON CERTIFICAZIONE NIAP 3.0**

						
N. ARTICOLO	SS2P-SH-DP-U/ SS2P-SH-DP-UCAC	SS4P-SH-DP-U/ SS4P-SH-DP-UCAC	SS8P-SH-DP-U/ SS8P-SH-DP-UCAC	SS2P-DH-DP-U/ SS2P-DH-DP-UCAC	SS4P-DH-DP-U/ SS4P-DH-DP-UCAC	SS4P-QH-DP-UCAC
Descrizione	Switch KVM sicuro a 2 porte, utente singolo, DisplayPort 4K single-head	Switch KVM sicuro a 4 porte, utente singolo, DisplayPort 4K single-head	Switch KVM sicuro a 8 porte, utente singolo, DisplayPort 4K single-head	Switch KVM sicuro a 2 porte, utente singolo, DisplayPort 4K dual-head	Switch KVM sicuro a 4 porte, utente singolo, DisplayPort 4K dual-head	Switch KVM sicuro a 4 porte, utente singolo, DisplayPort 4K quad-head
N. di sorgenti (max.)	2	4	8	2	4	4
Compatibilità del computer	Windows, Mac e Linux OS					
Risoluzione max.	4K fino a 3840 x 2160 a 30 Hz					
Compatibilità del monitor	La maggior parte dei monitor mediante emulazione ed EDID learning sicuri					
<b>PORTE ALLA CONSOLE UTENTE</b>						
Connessione/i monitor	1x DisplayPort 1.2		2x DisplayPort 1.2		4x DisplayPort 1.2	
Connessioni di tastiera e mouse	2x USB 1.1 Tipo A, solo tastiera e mouse					
Uscita audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching					
Supporto CAC (solo modelli UCAC)	1x USB Tipo A, interamente configurabile					
<b>PORTE AI COMPUTER</b>						
Ingresso/i video	1x DisplayPort 1.2 per sorgente		2x DisplayPort 1.2 per sorgente		4x DisplayPort 1.2 per sorgente	
Ingresso tastiera e mouse	1x USB 1.1 Tipo B con emulazione USB per sorgente					
Ingresso audio	1x jack audio da 3,5 mm per sorgente					
Supporto CAC (solo modelli UCAC)	1x USB Tipo B per sorgente					

**SWITCH KVM HDMI SICURI, CON CERTIFICAZIONE NIAP 3.0**

				
N. ARTICOLO	SS2P-SH-HDMI-U/ SS2P-SH-HDMI-UCAC	SS4P-SH-HDMI-U/ SS4P-SH-HDMI-UCAC	SS2P-DH-HDMI-U/ SS2P-DH-HDMI-UCAC	SS4P-DH-HDMI-U/ SS4P-DH-HDMI-UCAC
Descrizione	Switch KVM sicuro a 2 porte, utente singolo, HDMI 4K single-head	Switch KVM sicuro a 4 porte, utente singolo, HDMI 4K single-head	Switch KVM sicuro a 2 porte, utente singolo, HDMI 4K dual-head	Switch KVM sicuro a 4 porte, utente singolo, HDMI 4K dual-head
N. di sorgenti (max.)	2	4	2	4
Compatibilità del computer	Windows, Mac e Linux OS			
Risoluzione max.	4K fino a 3840 x 2160 a 30 Hz			
Compatibilità del monitor	La maggior parte dei monitor mediante emulazione ed EDID learning sicuri			
<b>PORTE ALLA CONSOLE UTENTE:</b>				
Connessione/i monitor	1x HDMI 1.4		2x HDMI 1.4	
Connessioni di tastiera e mouse	2x USB 1.1 Tipo A, solo tastiera e mouse			
Uscita audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching			
Supporto CAC (solo modelli UCAC)	1x USB Tipo A, interamente configurabile			
<b>PORTE AI COMPUTER:</b>				
Ingresso/i video	1x HDMI 1.4 per sorgente		2x HDMI 1.4 per sorgente	
Connessioni di tastiera e mouse	1x USB 1.1 Tipo B con emulazione USB per sorgente			
Ingresso audio	1x jack audio da 3,5 mm per sorgente			
Supporto CAC (solo modelli UCAC)	1x USB Tipo B per sorgente			

**SWITCH KVM SICURI DVI-I (VGA MEDIANTE ADATTATORE), CON CERTIFICAZIONE NIAP 3.0**

								
N. ARTICOLO	SS2P-SH-DVI-U/ SS2P-SH-DVI-UCAC	SS4P-SH-DVI-U/ SS4P-SH-DVI-UCAC	SS8P-SH-DVI-U/ SS8P-SH-DVI-UCAC	SS16P-SH-DVI-UCAC	SS2P-DH-DVI-U/ SS2P-DH-DVI-UCAC	SS4P-DH-DVI-U/ SS4P-DH-DVI-UCAC	SS8P-DH-DVI-UCAC	SS4P-QH-DVI-UCAC
Descrizione	Switch KVM sicuro a 2 porte, utente singolo, DVI-I single-head	Switch KVM sicuro a 4 porte, utente singolo, DVI-I single-head	Switch KVM sicuro a 8 porte, utente singolo, DVI-I single-head	Switch KVM sicuro a 16 porte, utente singolo, DVI-I single-head	Switch KVM sicuro a 2 porte, utente singolo, DVI-I dual-head	Switch KVM sicuro a 4 porte, utente singolo, DVI-I dual-head	Switch KVM sicuro a 8 porte, utente singolo, DVI-I dual-head	Switch KVM sicuro a 4 porte, utente singolo, DVI-I quad-head
N. di sorgenti (max.)	2	4	8	16	2	4	8	4
Compatibilità del computer	Windows, Mac e Linux OS							
Risoluzione max.	2560 x 1600 a 60 Hz							
Compatibilità del monitor	La maggior parte dei monitor mediante emulazione ed EDID learning sicuri							
<b>PORTE ALLA CONSOLE UTENTE:</b>								
Connessione/i monitor	1x DVI-I			2x DVI-I			4x DVI-I	
Connessioni di tastiera e mouse	2x USB 1.1 Tipo A, solo tastiera e mouse							
Uscita audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching							
Supporto CAC (solo modelli UCAC)	1x USB Tipo A, interamente configurabile							
<b>PORTE AI COMPUTER:</b>								
Ingresso/i video	1x DVI-I per sorgente			2x DVI-I per sorgente			4x DVI-I per sorgente	
Tastiera e mouse	1x USB 1.1 Tipo B con emulazione USB, 2x PS/2 miniDIN6 per sorgente							
Ingresso audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching per sorgente							
Supporto CAC (solo modelli UCAC)	1x USB Tipo B per sorgente							

	<b>MULTIVIEWER NIAP CON CERTIFICAZIONE NIAP 3.0</b>	<b>DISPOSITIVO DI PROTEZIONE PERIFERICHE NIAP 3.0</b>
		
N. ARTICOLO	SS4P-SH-DVI-UCAC-P	SS1P-DVI-UCAC-P
Descrizione	Switch KVM sicuro a 4 porte, DVI-I con sistema multiview 4-in-1	Dispositivo di protezione periferiche sicuro a 1 porta
N. di sorgenti (max.)	4	1 periferica
Connessioni monitor per console	2	N/A
Risoluzione max.	2560 x 1600 a 60 Hz	2560 x 1600 a 60 Hz
<b>PORTE ALLA CONSOLE UTENTE:</b>		<b>PORTE PERIFERICHE:</b>
Connessione/i monitor	2x DVI-I (1x schermo intero, 1x vista a quattro sorgenti)	1x DVI-I
Connessioni di tastiera e mouse	2x USB 1.1 Tipo A	2x USB 1.1 Tipo A
Uscita audio	1x jack audio da 3,5 mm	x jack audio da 3,5 mm
Supporto CAC	1x config. USB Tipo A	1x config. USB Tipo A
<b>PORTE AI COMPUTER:</b>		
Ingresso/i video	1x DVI-I per sorgente	1x DVI-I
Connessioni di tastiera e mouse	1x USB 1.1 Tipo B emulato per sorgente	1x USB 1.1 Tipo B emulato
Ingresso audio	1x jack audio da 3,5 mm per sorgente	1x jack audio da 3,5 mm
Supporto CAC - solo modelli UCAC	1x USB Tipo B per sorgente	1x USB Tipo B



	SWITCH A MATRICE KVM DVI-I CON CERTIFICAZIONE NIAP 3.0				SWITCH KM, NIAP 3.0 NESSUNA PORTA VIDEO ATTIVATA	
						
N. ARTICOLO	SS4P-DVI-4X2-UCAC	SS8P-DVI-8X2-UCAC	SS4P-DVI-4X4-UCAC	SS8P-DVI-8X4-UCAC	SS4P-KM-U/ SS4P-KM-UCAC	SS8P-KM-U/ SS8P-KM-U
Descrizione	4x2 switch a matrice KVM sicuri, DVI-I	8x2 switch a matrice KVM sicuri, DVI-I	4x4 switch a matrice KVM sicuri, DVI-I	8x4 switch a matrice KVM sicuri, DVI-I	Switch KM sicuro a 4 porte, utente singolo	Switch KM sicuro a 8 porte, utente singolo
N. di sorgenti (max.)	4	8	4	8	4	8
Compatibilità del computer	Computer con Windows, Mac e Linux OS				Windows, Mac e Linux OS	
N. di utenti	2	2	4	4	1	1
Monitor della console	1	1	1	1	N/A	
Risoluzione max.	2560 x 1600 a 60 Hz				N/A	
Compatibilità del monitor	La maggior parte dei monitor mediante emulazione ed EDID learning sicuri				N/A	

#### PORTE ALLA CONSOLE UTENTE:

Connessione monitor	1x DVI-I per console	N/A, i monitor mantengono una connessione diretta con il computer
Connessioni di tastiera e mouse	2x USB 1.1 Tipo A, solo tastiera e mouse per console	2x USB 1.1 Tipo A, solo tastiera e mouse
Uscita audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching per sorgente	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching
Supporto CAC	1x USB Tipo A, interamente configurabile per console	1x USB Tipo A, interamente configurabile

#### PORTE AI COMPUTER:

Ingressi video	1x DVI-I per sorgente	N/A
Connessioni di tastiera e mouse	1x USB 1.1 Tipo B con emulazione USB per sorgente	1x USB 1.1 Tipo B con emulazione USB per sorgente
Ingresso audio	1 jack audio da 3,5 mm con uscite altoparlanti bilanciate e switching per sorgente	1x jack audio da 3,5 mm per sorgente
Supporto CAC (solo modelli UCAC)	1x USB tipo B per sorgente	1x USB tipo B per sorgente

#### ACCESSORI

Cavi per switch KVM sicuro	
SKVMCBL-DP-06	DisplayPort, USB, 3,5 mm audio; 1,8 m
SKVMCBL-HDMI-06	HDMI, USB, 3,5 mm audio; 1,8 m
SKVMCBL-DVI-06	DVI, USB, 3,5 mm audio; 1,8 m

## CONTATTA BLACK BOX

Non sei sicuro di quello che ti serve?

Contatta i nostri esperti KVM.

Chiama il numero 00800-2255 2269

oppure visita il sito [WWW.BLACK-BOX.EU/TSC](http://WWW.BLACK-BOX.EU/TSC).



## PERCHÉ BLACK BOX?

### ESPERIENZA

I project engineer di Black Box sono a disposizione per assisterti nella valutazione, progettazione, installazione e formazione del sistema.

### PORTATA

Black Box offre la gamma più completa di soluzioni KVM di tutto il settore.

### SUPPORTO

A sostegno dell'impegno da noi dedicato a garantire la totale soddisfazione, il nostro team dedicato di tecnici altamente qualificati è a disposizione per consulenze telefoniche gratuite tutti i giorni dell'anno.

### GARANZIE

Gli switch KVM sicuri sono coperti da una garanzia di 3 anni e sono disponibili opzioni di estensione.

### FORZA FINANZIARIA

Fatturato annuo di quasi 1 miliardo \$; quotazione in borsa (BBOX).

### ESPERIENZA

Fornitore leader di soluzioni tecnologiche fin dal 1976, Black Box aiuta oltre 175.000 clienti in 150 paesi a costruire, gestire, ottimizzare e mettere in sicurezza infrastrutture IT.

### CENTRO DI ECCELLENZA

Black Box mette a disposizione un centro di eccellenza che offre servizi professionali e accordi di supporto finalizzati a ottimizzare i sistemi dei clienti e massimizzare l'uptime.

### ACCORDI SUI LIVELLI DI SERVIZIO

I nostri Accordi sui livelli di servizio consentono ai clienti di accedere ad assistenza tecnica, formazione sui prodotti, application engineer dedicati e molto altro ancora.