BLACK BOX®

BROSCHÜRE
KVM-TECHNOLOGIE

Secure KVM Switches

Broschüre

MEHR ERFAHREN BLACKBOX.COM/SECUREKVM

Wehren Sie verschiedene Sicherheitsbedrohungen ab, die bei der gemeinsamen Nutzung von Peripheriegeräten in Computernetzwerken mit unterschiedlichen Sicherheitsstufen auftreten können

Warum Secure KVM

Cyber-Bedrohungen entwickeln sich ständig weiter und werden immer häufiger und raffinierter. Unsere Abhängigkeit von der Technologie, die gemeinsame Nutzung globaler Ressourcen und der Bedarf an Echtzeit-Zusammenarbeit haben zu einem wachsenden Netz von Daten und deren Abhängigkeit voneinander geführt. Die Vernetzung hilft uns zwar, effizienter und effektiver zusammenzuarbeiten, aber sie macht uns auch zunehmend anfällig für verheerende Cyberangriffe.

Sowohl große Verteidigungsbehörden als auch andere Organisationen setzen fortschrittliche Sicherheitsmaßnahmen ein, um Netzwerke zu isolieren und Informationen vor Bedrohungen von außen zu schützen. Es gibt jedoch einen Ort, an dem isolierte Netzwerke und sensible Informationen zusammenkommen: der Benutzer-Desktop.

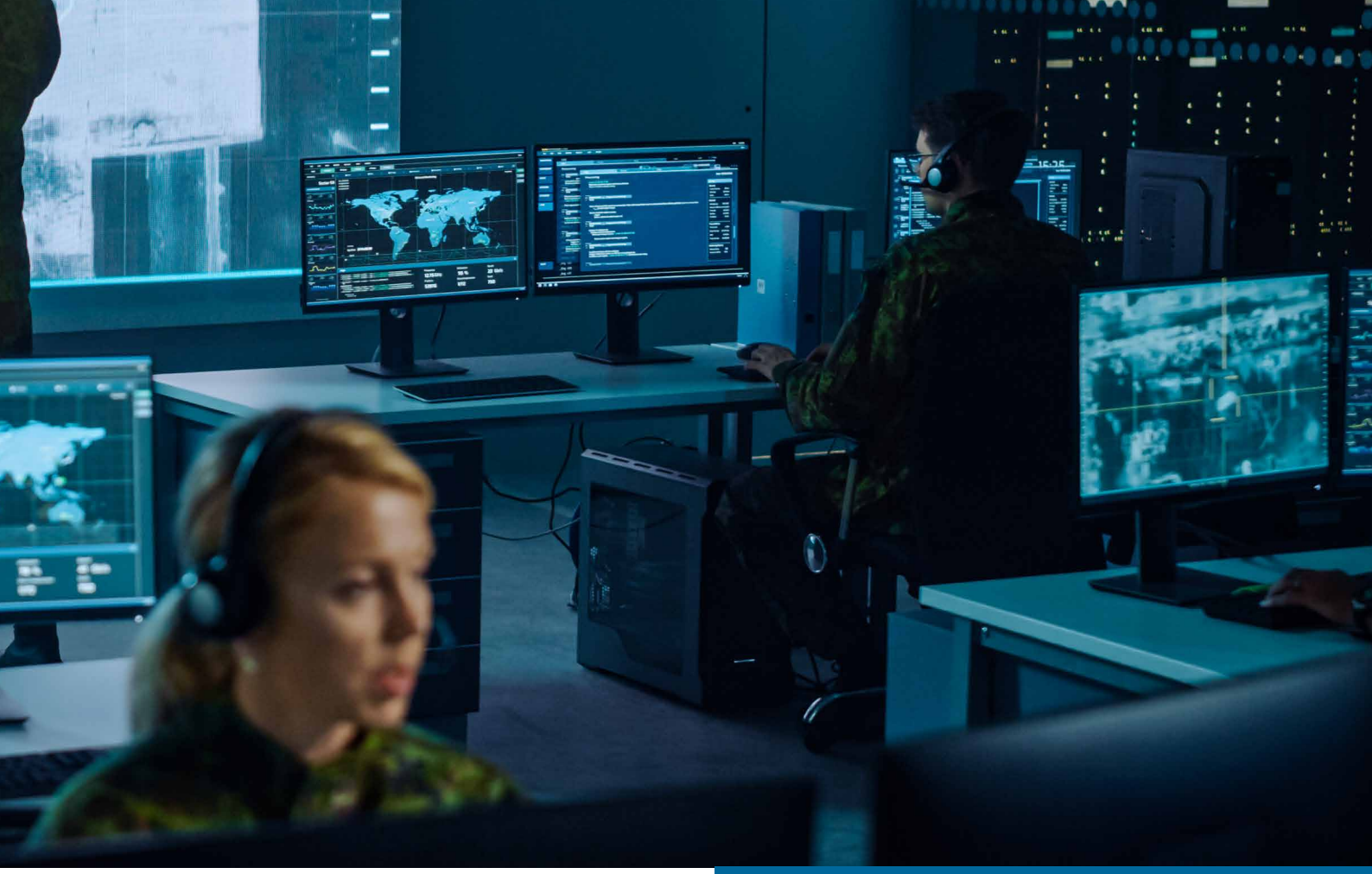
Herkömmliche KVM-Switches sind anfällig für Cyberangriffe und können Cyberkriminellen den Zugriff auf vertrauliche Daten ermöglichen. Wenn ein Cyberkrimineller Informationen von einem als geheim klassifizierten Server stehlen möchte, kann er ein USB-Laufwerk mit Malware oder einem Virus darauf an einen regulären KVM-Switch anschließen und so auf mehrere Server statt nur auf einen zugreifen. Herkömmliche KVM-Switches sind auch anfälliger für die böswillige Nutzung von LCD-Monitoren (über das EDID-Signal), Mikrofonen oder CAC-Geräten.

Durch diese Methoden kann eine Fülle von Verschlusssachen in die falschen Hände geraten und zum Schaden der Organisation verwendet werden.

Herkömmliche KVM-Switches

KVM-Switches ermöglichen den Zugriff auf und die Verwaltung von mehreren Computern von einem einzigen Arbeitsplatz mit jeweils einer Tastatur, Maus und einem oder mehreren Bildschirmen. Benutzer können auf Knopfdruck oder per Tastendruck problemlos auf Informationen und Anwendungen auf völlig getrennten Systemen zugreifen.

Die KVM-Technologie bietet Überwachungslösungen für Automatisierung, Prozesse und Arbeitsabläufe. Sie bietet den Benutzern eine bessere Bedienbarkeit und eine schnelle Amortisierung der Investition durch eine bessere Ergonomie und Produktivität am Arbeitsplatz. Mit KVM-Switches können Benutzer durch die Reduzierung von Schnittstellengeräten Platz sparen, durch den Wegfall redundanter Peripheriegeräte Kosten sparen und in kritischen Situationen schneller reagieren.



Beispiele für Anwendungsfälle

Secure KVM-Switches schützen sensible Daten

Ein Secure KVM-Switch ist ein Desktop-Switch mit 2, 4 oder 8 Anschlüssen, der die Steuerung und Trennung von PCs ermöglicht, die mit Netzwerken unterschiedlicher Sicherheitseinstufungen verbunden sind. Im Gegensatz zu herkömmlichen KVM-Switches können Secure KVM-Switches nur über Drucktasten gesteuert werden. Hotkey-Befehle sind deaktiviert, so dass nur lokale, ausgewählte Benutzer Zugriff haben.

Secure KVM-Switches lassen nicht zu, dass ein nicht erkanntes USB-Laufwerk auf Informationen zugreift. Administratoren können wählen, welche USB-Geräte zugelassen oder erkannt werden sollen. Secure KVM-Switches leisten noch viel mehr, um Behörden vor den schrecklichsten Cyberbedrohungen zu schützen, die es heute gibt.

Common Criteria

NIAP

TAA COMPLIANT

NIAP-Schutzprofil für Secure KVM

Bis vor kurzem verwendete die National Information Assurance Partnership (NIAP) das Common Criteria Evaluation & Validation Scheme (CCEVS), um KVM-Switches hinsichtlich ihrer Sicherheit zu bewerten und zu genehmigen.

Das NIAP hat das "Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement" für die Anwendung der Gemeinsamen Kriterien umgesetzt und evaluiert nicht mehr anhand von "Evaluation Assurance Levels" (EAL). Dies stärkt die Evaluierung durch die Konzentration auf technologiespezifische Sicherheitsanforderungen.

Infolgedessen wurde das Protection Profile (PP) für Peripheral Sharing Switches auf PP 4.0 NIAP Protection Profile for Peripheral Sharing Switch Version 4.0 aktualisiert, bei dem es sich um Tests für den Prozess der Entwicklung, Prüfung, Verifizierung und Auslieferung von Sicherheitsprodukten handelt. Dieses Schutzprofil ist ein internationales, standardisiertes Verfahren zur Bewertung, Validierung und Zertifizierung der Sicherheit von Informationstechnologien.

Wie sichere KVM-Switches Cyberangriffe abwehren

Strenge Sicherheitsmerkmale von Black Box Secure KVM-Switches

- Mechanische, elektrische und optische Signalisolierung verhindern Hackerangriffe und Datenverluste -> absolute Isolierung / kein Datenverlust zwischen sicheren Ports und der Außenwelt
- Geschützte Firmware verhindert, dass Eindringlinge die Firmware umprogrammieren oder auslesen (nicht umprogrammierbares ROM)
- Opto-Isolierte USB-Ports und Tastatur-/interne Cache-Löschung sorgen dafür, dass die USB-Datenpfade elektrisch voneinander isoliert sind, um USB-Datenverluste zwischen den Ports zu verhindern
- Die sichere EDID-/Video- und Aux-Emulation schränkt die Erkennung neu angeschlossener Bildschirme bei Umschaltvorgängen ein und verhindert so, dass unerwünschte und ungesicherte Daten zwischen Computer und Bildschirm übertragen werden.
- Schutz vor Einbruch in das Gehäuse: ausgestattet mit aktiven Manipulationsschutzschaltern und externen Hologramm-Siegeln, die eine Manipulation verhindern
- Optionale konfigurierbare Common Access Card (CAC)-Unterstützung für Smartcards, biometrische Leser und die Registrierung externer USB-Geräte
- Unidirektionaler Datenfluss zu speziellen Peripheriegeräten wie einem Projektor, Drucker oder Audiosystem
- Zertifiziert nach NIAP PP 4.0, der höchsten Stufe der Common Criteria (Protection Profile for Peripheral Sharing Switch Version 4.0)
- TAA-konform und in den USA hergestellt
- Audioeingang ist zulässig, aber nur, wenn keine anderen Peripheriegeräte vom Switch unterstützt werden (Mikrofon kann nicht mit Lautsprechern koexistieren)

Getestet und zertifiziert nach dem neuesten Sicherheitsprofil NIAP PP 4.0

Secure KVM-Switches von Black Box sind für den Einsatz in sicheren Verteidigungs- und Geheimdienstanwendungen konzipiert, bei denen sensible Daten geschützt werden müssen. Sie sind NIAP PP 4.0-zertifiziert und mit den höchsten Sicherheitsmerkmalen ausgestattet, die den heutigen Standards für die sichere Kontrolle von Informationen entsprechen. Die Switches verfügen über einzigartige Hardwarekonfigurationen, die einen Datenaustausch zwischen PCs und angeschlossenen Peripheriegeräten verhindern und somit jegliche potenzielle Cyberbedrohung ausschließen. NIAP PP 4.0 verwendet ein Basisschutzprofil mit individuellen Modulen für Peripherietypen.

Mehrstufige Sicherheit für strenge Informationssicherheit

Eine absolute Isolierung der mechanischen, elektrischen und optischen Signale durch Luftschleusen verhindert Hackerangriffe und Datenverluste zwischen den Anschlüssen und der Außenwelt. Jeder Anschluss des Secure KVM-Switches verwendet seine eigenen isolierten Datenkanäle. Bevor der KVM-Switch sich auf einen anderen Zielcomputer aufschaltet, löscht er den internen Cache und die Tastaturdaten, um sicherzustellen, dass keine Restdaten im Kanal verbleiben. Firmware und ROM sind nicht umprogrammierbar und verhindern, dass Eindringlinge die Daten lesen, durch unerwünschte Firmware-Upgrades umprogrammieren oder sensible Daten physisch entfernen.

Schutz vor dem Eindringen in das Gehäuse

Secure KVM-Switches verfügen über manipulationssichere Gehäuse, externe Hologramm-Siegel und eine langlebige, interne, manipulationssichere Batterie. Wenn die Abdeckung vom Gehäuse entfernt wird, unterbricht der KVM-Switch die Verbindung mit allen angeschlossenen PCs und Peripheriegeräten und deaktiviert alle Funktionen, um jeden Versuch eines physischen Eindringens zu verhindern. Die Manipulationserkennung ist in V4.0 optional (in V3.0 ist sie obligatorisch), da einige Geräte über austauschbare Karten für verschiedene Peripheriegeräte verfügen können (in diesem Fall sind Manipulationssiegel ausreichend). V3.0 verbietet die Audioeingabe (Mikrofon), während V4.0 die Audioeingabe zulässt (aber nur, wenn das Gerät keine anderen Peripheriegeräte unterstützt, z. B. kann ein Mikrofon nicht mit Lautsprechern koexistieren).

Tastatur- und Maus-Emulation

Secure KVM-Switches emulieren das Vorhandensein einer Tastatur und Maus für jeden angeschlossenen Computer über ein USB-Kabel. Sowohl ausgewählte als auch nicht ausgewählte Computer halten eine konstante Verbindung mit den Tastatur-Maus-Emulations-Controllern des Switches aufrecht, was ein extrem schnelles Umschalten ermöglicht und die Erkennung neu angeschlossener Peripheriegeräte während des Umschaltvorgangs einschränkt. Die Emulation von Tastatur und Maus verhindert auch eine direkte Verbindung zwischen den Peripheriegeräten und den angeschlossenen Computern, wodurch die Systeme vor potenziellen Sicherheitslücken geschützt werden. PS/2-Anschlüsse sind in V3.0 erlaubt und ab V4.0 ausgeschlossen.

Vollständig konfigurierbarer Common Access Card (CAC)-Anschluss für externe USB-Peripheriegeräte

Viele Secure KVM-Switches unterstützen CAC-Geräte (Common Access Card), z. B. Smartcard- und biometrische Lesegeräte, die die Sicherheit bei der Verwendung des Geräts erhöhen. Black Box geht jedoch noch einen Schritt weiter und ermöglicht es authentifizierten Administratoren, bestimmte Peripheriegeräte zu registrieren und dem CAC-Port zuzuweisen (optional). Benutzer können dann zugewiesene Geräte auf die jeweilig angeschlossenen Computer aufschalten.

Schränkt neue Monitorverbindungen während der Umschaltung ein

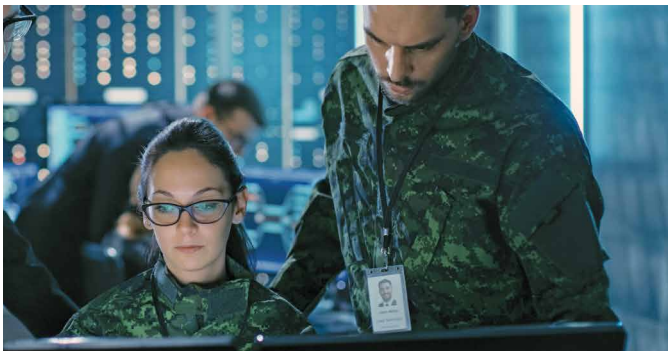
Secure KVM-Switches simulieren standardmäßig eine generische EDID, so dass sie eine Vielzahl an Bildschirmen unterstützen. Ausgewählte und nicht ausgewählte Computer stehen in ständiger Verbindung mit den Video- und AUX-Emulationscontrollern des Switches, was ein extrem schnelles Umschalten ermöglicht und die Erkennung neu angeschlossener Monitore während des Umschaltvorgangs einschränkt. Dies schützt die Systeme vor potenziellen Schwachstellen durch unerwünschte und unsichere Datenübertragungen über DDC-Leitungen. V.4.0 erlaubt die Verwendung von Multiviewern (diese müssen jedoch OSD verwenden, um den/die aktiven Videokanal/Kanäle zu identifizieren).

Use Cases

Ideal für viele Branchen

- Öffentliche Einrichtungen
- Verteidigung & Militär
- Kontrollräume für das Verkehrsmanagement
- Bankwesen und Finanzen
- Bildungswesen
- Gesundheitswesen
- F&E-Abteilungen
- Versorgungsunternehmen

Use Cases

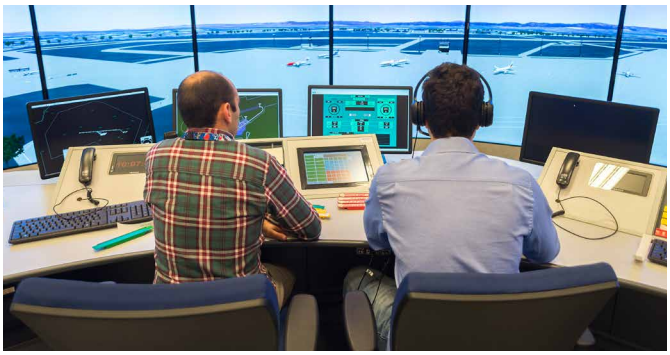


Defense Communications Center

Ein Kunde aus dem Verteidigungsbereich wandte sich mit zwei dringenden Problemen an Black Box: ineffizienter Netzwerkzugang sowie unübersichtliche Bediener-Arbeitsplätze.

Die Bediener mussten auf mehrere Computernetzwerke von einem sicherem Kommunikationszentrum aus zugreifen. Das war ein zeitaufwändiger Prozess, da für jedes Computernetzwerk eine eigene Tastatur, ein eigener Monitor und eine eigene Maus erforderlich waren, was bedeutete, dass sich der Bediener zwischen den verschiedenen Systemen bewegen musste, um auf sensible Daten und Geheimdienstnetzwerke zuzugreifen. Dies erforderte auch einen Tisch für alle sechs verschiedenen Monitore, sechs verschiedene Tastaturen und sechs verschiedene Mäuse, was zu einem unübersichtlichen und beengten Arbeitsbereich führte.

Um diese Herausforderungen zu meistern, wurde ein 8-Port Secure KVM-Switch von Black Box implementiert, der die Konfiguration auf einen Monitor, eine Tastatur und eine Maus reduzierte. Dies sparte den Mitarbeitern wertvolle Zeit für das Wechseln zwischen mehreren Netzwerken und Reduzierte eine Vielzahl an Geräten auf den jeweiligen Schreibtischen. Heute können die Bediener effizienter arbeiten und gleichzeitig sicherstellen, dass ihre wichtigen Daten nicht in Gefahr geraten.



Polizei

Ein Integrator wandte sich an Black Box, als es eine hochsichere Lösung für ein Polizeiprojekt benötigt wurde. Die Projektingenieure mussten das Schalten zwischen einem offenen (grünen) und einem sicheren (roten) Netz ermöglichen. Black Box schlug den 4-Port DVI USB Secure KVM-Switch vor, der alle Anforderungen erfüllt. Mehr als 1.000 Secure KVM-Switches wurden für dieses Projekt bis heute installiert.

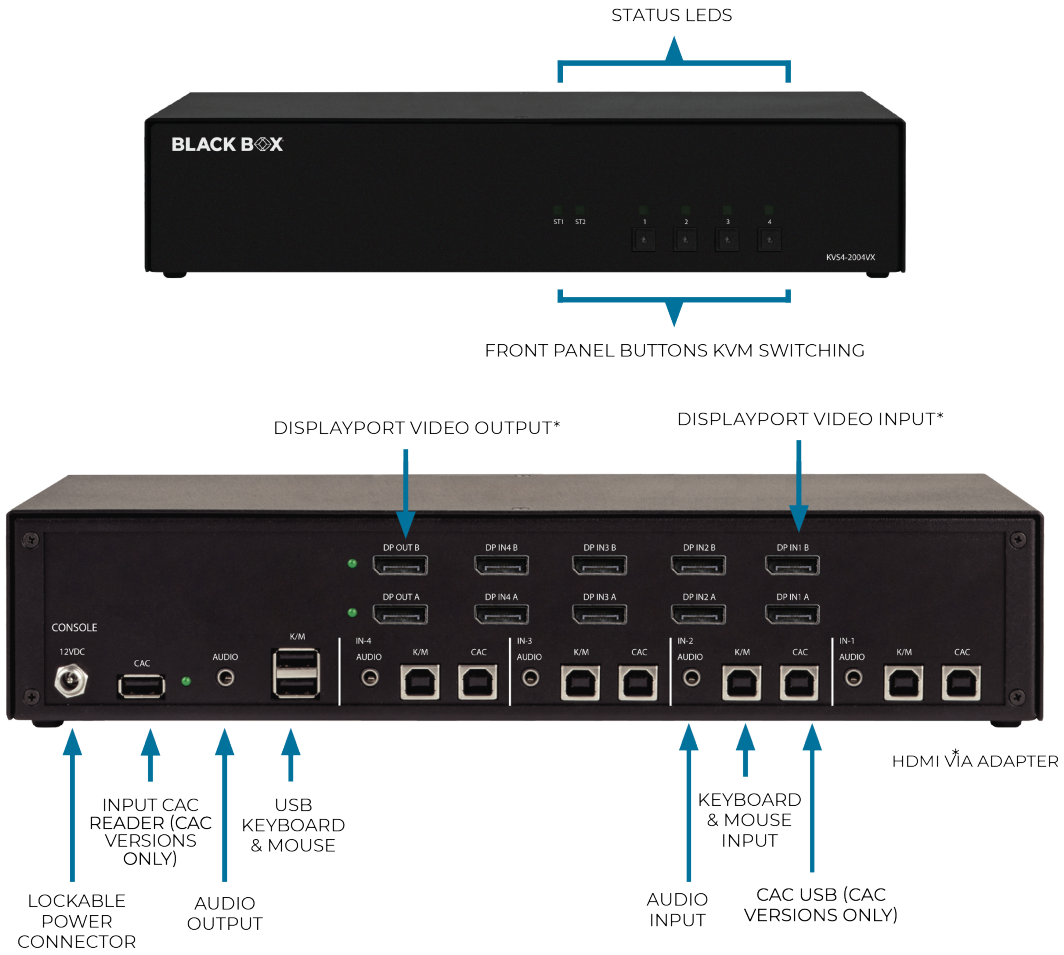
Unternehmensbereich

Die gemeinsame Nutzung globaler Ressourcen und der Bedarf an Echtzeit-Zusammenarbeit haben zu einem immer größeren Netz von Daten geführt. Die Vernetzung hilft Organisationen zwar, effizienter und effektiver zusammenzuarbeiten, macht sie aber auch zunehmend anfällig für verheerende Cyberangriffe. Schließlich müssen Systeme, die auf das Internet zugreifen, von anderen Systemen ferngehalten werden, die für sensible Unternehmens- oder persönliche Daten verwendet werden. Um ihre Informationssicherheit zu gewährleisten, ersetzen viele Unternehmen herkömmliche KVM-Switches durch Secure KVM-Switches.

Secure KVM-Produktübersicht

Secure KVM-Switch-Design

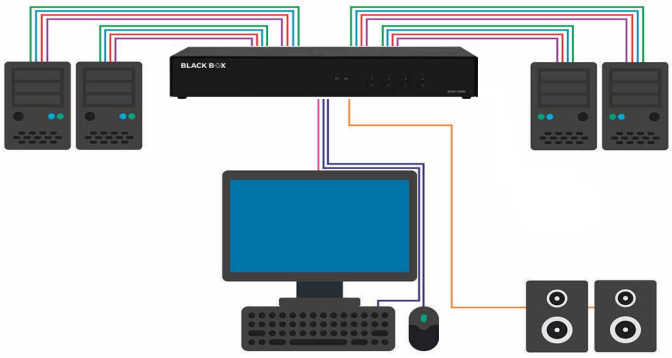
Beispiel: 4-Port Secure KVM-Switch, Einzelbenutzer, DisplayPort, USB und CAC KVS4-2004VX



Secure, NIAP 4.0-zertifizierte Desktop-KVM-Switch-Typen

Secure Desktop-KVM-Switches, Einzelbenutzer

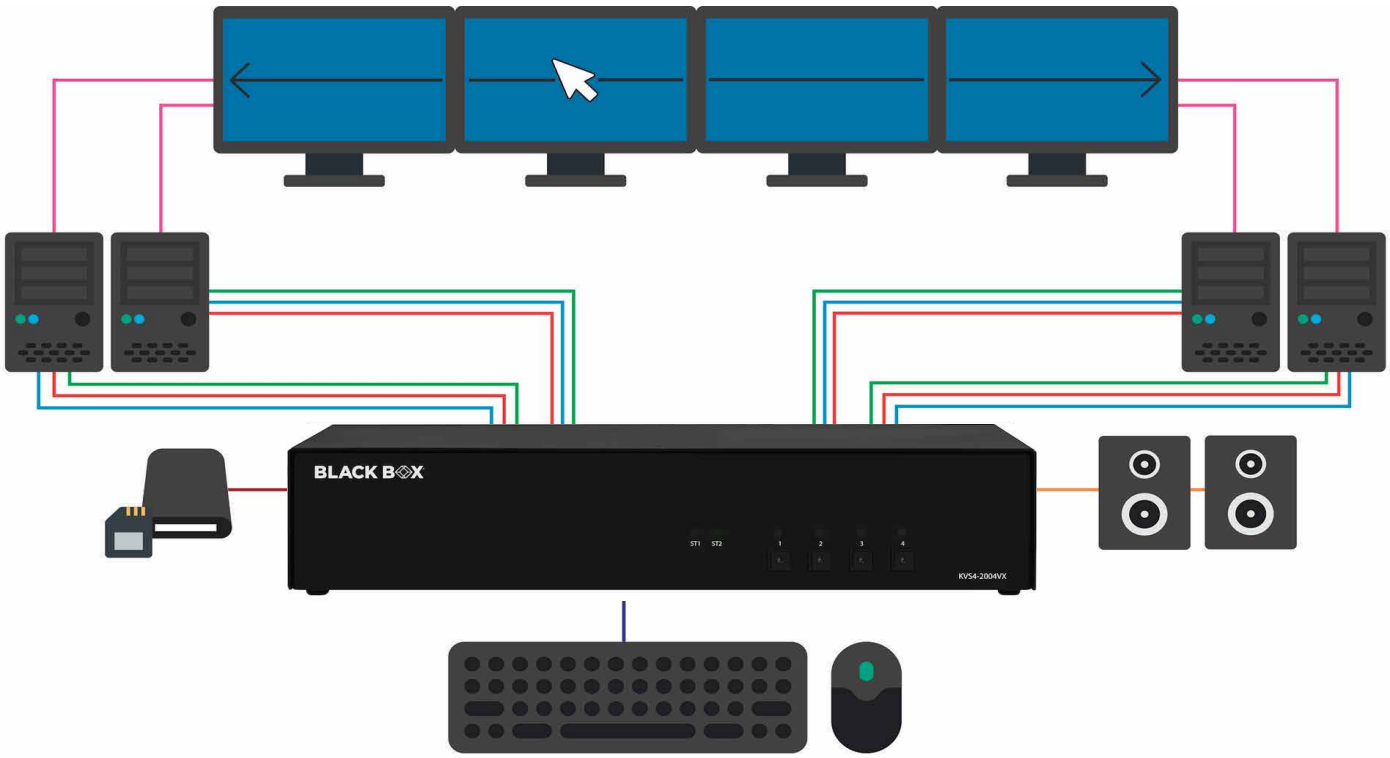
- Geteilter Zugriff auf zwei, vier oder acht Computer von einer einzigen Benutzerkonsole aus
- Verfügbar mit DVI-I-, DisplayPort- oder HDMI/DisplayPort-Video
- Hochwertiges DisplayPort 1.2/HDMI-Video mit Auflösungen bis zu 4K@60Hz und beste DVI-I Dual-Link-Auflösung bis zu 2560x1600@60Hz
- Wählen Sie zwischen Modellen mit Einzel-, Doppel- oder Vierfach-Monitoranschlüssen an der Konsole
- USB-Tastatur/Maus plus Stereo-Audio
- Erhältlich mit oder ohne CAC-Unterstützung
- Hergestellt, getestet und zertifiziert in den USA



Finden Sie das passende Produkt mit dem Selektor auf den Seiten 9 und 10.

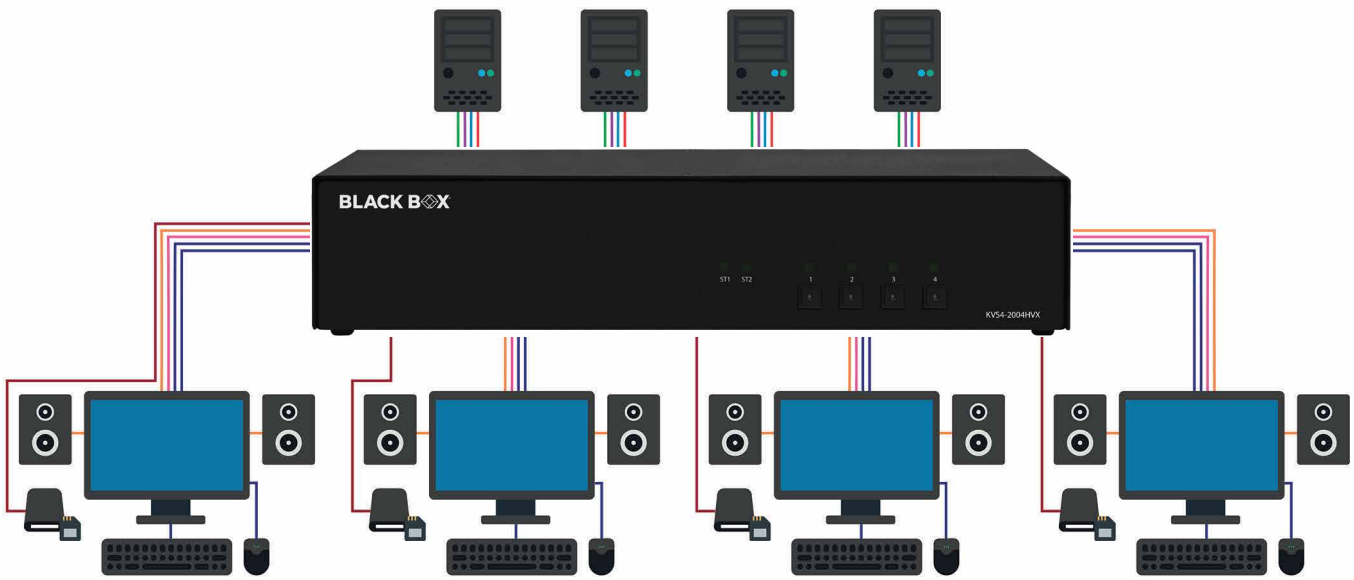
Sichere NIAP 4.0-zertifizierte KM-Switches

- Umschalten durch Bewegen der Maus von Monitor zu Monitor (Glide & Switch)
- Gleichzeitige Anzeige mehrerer Quellen über spezielle Computer-/Monitorverbindungen
- Unterstützung von Stereo-Audio
- Geteilter Zugriff auf vier oder acht Computer von einer einzigen Benutzerkonsole aus via USB-Tastatur und -Maus
- Unterstützung von Stereo-Audio
- Erhältlich mit oder ohne CAC-Unterstützung
- Hergestellt, getestet und zertifiziert in den USA



Sicherer NIAP 4.0-zertifizierter KVM-Switch - FlexPort HDMI/DisplayPort

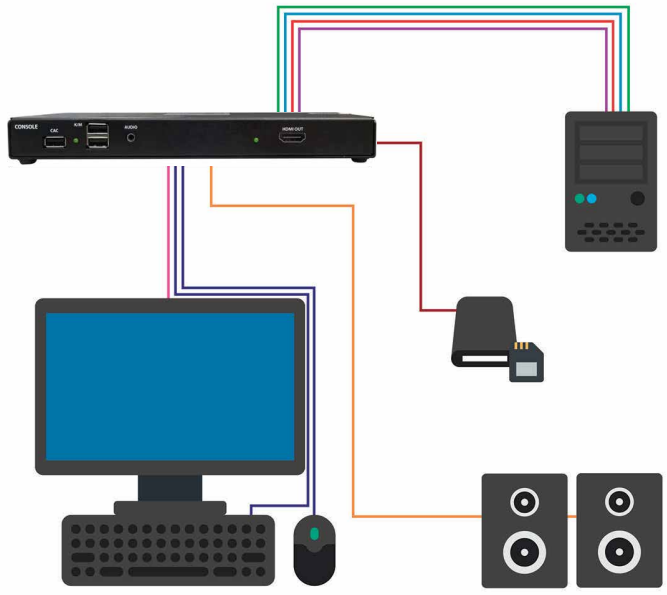
- Sicherer Zugriff auf zwei oder bis zu vier Computern (Tastatur-, Video- und Maus) mit einem oder zwei HDMI/ DisplayPort-Monitoren dank FlexPort-Technologie
- Zertifiziert für NIAP-Schutzprofil für Peripheriegeräte mit gemeinsamer Nutzung, Version 4.0
- Unterstützt Auflösungen bis zu 4K@60Hz
- Hergestellt, getestet und zertifiziert in den USA
- Externe Stromversorgung



Finden Sie das passende Produkt mit dem Selektor auf den Seiten 9 und 10.

Secure KVM-Peripherie-Defender, NIAP 4.0 zertifiziert - CAC

- Isoliert einen Computer von DVI-I-, HDMI- oder DisplayPort-Signalen, sowie Tastatur, Maus und CAC Steuersignalen, um eine erhöhte Sicherheit zu gewährleisten.
- Zertifiziert für NIAP-Schutzprofil für Peripheriegeräte mit gemeinsamer Nutzung, Version 4.0
- Einzelmonitor-Videoschnittstelle
- Verbesserter Schutz für ungesicherte Peripheriegeräte
- Getestet und zertifiziert nach dem US-amerikanischen Standard
- Externe Stromversorgung
- Gewährleistet unidirektionalen Datenfluss von Video, USB und Audio vom Computer zum Peripheriegerät
- Unterstützt die meisten Monitore durch Secure EDID Learning/ Emulation
- Ideal bspw. für Konferenzräume, um Laptops vor unerwünschten Zugriffen durch die gemeinsame Display-Verbindung zu schützen



Finden Sie das passende Produkt mit dem Selektor auf den Seiten 9 und 10.

NIAP 4.0 PRODUKTLÖSUNGEN

SECURE KVM-SWITCH, NIAP 4.0-ZERTIFIZIERT, DISPLAYPORT					
					
ARTIKEL #	KVS4-1004V	KVS4-2002V	KVS4-2004V	KVS4-2004VX	KVS4-2008VX
Beschreibung	2 Ports, Single-Monitor, DisplayPort	2 Ports, Dual-Monitor, DisplayPort	4 Ports, Dual-Monitor, DisplayPort	4 Ports, Dual-Monitor, DisplayPort, CAC	8 Ports, Dual-Monitor, DisplayPort, CAC
Anzahl der Quellen	2	2	4	4	8
System-Kompatibilität	Windows®, Mac®, und Linux® OS				
Max. Auflösung	Bis zu 4K@60Hz				
Monitor-Kompatibilität	Die meisten Monitore durch sicheres EDID-Lernen und Emulation				
ANSCHLÜSSE AM FÜR PERIPHERIEGERÄTE					
Monitorverbindung(en)	(1) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort
Tastatur/Maus-Verbindungen	(2) USB 2.0 Typ A, nur Tastatur und Maus				
Audio-Ausgang	(1) 3,5-mm-Audiobuchse mit symmetrischen Lautsprecherausgängen und Umschaltung				
CAC-Unterstützung	Nein	Nein	Nein	(1) USB Typ A, vollständig konfigurierbar	(1) USB Typ A, vollständig konfigurierbar
ANSCHLÜSSE ZU DEN COMPUTERN					
Monitorverbindung(en)	(1) DisplayPort pro Quelle	(2) DisplayPort pro Quelle	(2) DisplayPort pro Quelle	(2) DisplayPort pro Quelle	(2) DisplayPort pro Quelle
Tastatur/Maus-Verbindungen	(1) USB 2.0 Typ B mit USB-Emulation pro Quelle				
Audio-Ausgang	(1) 3,5-mm-Audiobuchse pro Quelle				
CAC-Unterstützung	Nein	Nein	Nein	(1) USB Typ B pro Quelle	(1) USB Typ B pro Quelle

SECURE KVM-SWITCH, NIAP 4.0-ZERTIFIZIERT, DVI-D					
					
ARTIKEL #	KVS4-1002D	KVS4-1004D	KVS4-2002D	KVS4-2004D	KVS4-2008D
Beschreibung	4 Ports, Single-Monitor, DVI-D	4 Ports, Single-Monitor, DVI-D	2 Ports, Dual-Monitor, DVI-D	4 Ports, Dual-Monitor, DVI-D	8 Ports, Dual-Monitor, DVI-D
Anzahl der Quellen	4	4	2	4	8
System-Kompatibilität	Windows®, Mac®, und Linux® OS				
Max. Auflösung	2560 x 1600 @ 60 Hz				
Monitor-Kompatibilität	Die meisten Monitore durch sicheres EDID-Lernen und Emulation				
ANSCHLÜSSE AM FÜR PERIPHERIEGERÄTE					
Monitorverbindung(en)	(1) DVI-D	(1) DVI-D	(2) DVI-D	(2) DVI-D	(2) DVI-D
Tastatur/Maus-Verbindungen	(2) USB 2.0 Typ A, nur Tastatur und Maus				
Audio-Ausgang	(1) 3,5-mm-Audiobuchse mit symmetrischen Lautsprecherausgängen und Umschaltung				
CAC-Unterstützung	Nein	Nein	Nein	Nein	Nein
ANSCHLÜSSE ZU DEN COMPUTERN					
Videoeingang(e)	(1) DVI-D pro Quelle	(1) DVI-D pro Quelle	(2) DVI-D pro Quelle	(2) DVI-D pro Quelle	(2) DVI-D pro Quelle
Tastatur/Maus-Eingaben	(1) USB 2.0 Typ B mit USB-Emulation pro Quelle				
Audio-Ausgang	(1) 3,5-mm-Audiobuchse pro Quelle				
CAC-Unterstützung	Nein	Nein	Nein	Nein	Nein

SECURE KVM-SWITCH, NIAP 4.0-ZERTIFIZIERT, FLEXPORT HDMI/DISPLAYPORT				
				
Artikel #	KVS4-1004HV	KVS4-2002HV	KVS4-2004HV	KVS4-2004HVX
Beschreibung	4 Ports, Einzelmonitor, FlexPort HDMI/DisplayPort	2 Ports, Dual-Monitor, FlexPort HDMI/DisplayPort	4 Ports, Dual-Monitor, FlexPort HDMI/DisplayPort	4 Ports, Dual-Monitor, FlexPort HDMI/DisplayPort, CAC
Anzahl der Quellen	4	2	4	4
System-Kompatibilität	Windows®, Mac®, und Linux® OS			
Max. Auflösung	Bis zu 4K@60Hz			
Monitor-Kompatibilität	Die meisten Monitore durch sicheres EDID-Lernen und Emulation			
ANSCHLÜSSE AM FÜR PERIPHERIEGERÄTE				
Monitorverbindung(en)	(1) HDMI/DisplayPort FlexPort	(2) HDMI/DisplayPort FlexPorts	(2) HDMI/DisplayPort FlexPorts	(2) HDMI/DisplayPort FlexPorts
Tastatur/Maus-Verbindungen	(2) USB 2.0 Typ A, nur Tastatur und Maus			
Audio-Ausgang	(1) 3,5-mm-Audiobuchse mit symmetrischen Lautsprecherausgängen und Umschaltung			
CAC-Unterstützung	Nein	Nein	Nein	(1) USB Typ A, vollständig konfigurierbar
ANSCHLÜSSE ZU DEN COMPUTERN				
Videoeingang(e)	(1) HDMI/DisplayPort FlexPort pro Quelle	(2) HDMI/DisplayPort FlexPorts pro Quelle	(2) HDMI/DisplayPort FlexPorts pro Quelle	(2) HDMI/DisplayPort FlexPorts pro Quelle
Tastatur/Maus-Eingaben	(1) USB 2.0 Typ B mit USB-Emulation pro Quelle			
Audio-Ausgang	(1) 3,5-mm-Audiobuchse pro Quelle			
CAC-Unterstützung	Nein	Nein	Nein	(1) USB Typ B pro Quelle

SECURE KVM-PERIPHERIE-DEFENDER, NIAP 4.0 ZERTIFIZIERT - CAC			
			
Artikel #	KVS4-8001DX	KVS4-8001HX	KVS4-8001VX
Beschreibung	DVI-D, CAC	HDMI, CAC	DisplayPort, CAC
System-Kompatibilität	Windows®, Mac®, und Linux® OS		
Max. Auflösung	2560 x 1600 @ 60Hz (DVI-D) Bis zu 4K @ 60Hz (HDMI- und DisplayPort-Modelle)		
Monitor-Kompatibilität	Die meisten Monitore durch sicheres EDID-Lernen und Emulation		
ANSCHLÜSSE AM FÜR PERIPHERIEGERÄTE			
Monitorverbindung(en)	(1) DVI-D 23-polig (Buchse)	(1) HDMI 1.4	(1) DisplayPort
Tastatur/Maus-Verbindungen	(2) USB Typ-A nur für Tastatur- und Mausanschluss (1) USB Typ-A für CAC-Anschluss	(2) USB Typ-A nur für Tastatur- und Mausanschluss (1) USB Typ-A für CAC-Anschluss	(2) USB Typ-A nur für Tastatur- und Mausanschluss (1) USB Typ-A für CAC-Anschluss
Audio-Ausgang	(1) Stereo 3,5-mm-Buchse	(1) Stereo 3,5-mm-Buchse	(1) Stereo 3,5-mm-Buchse
CAC-Unterstützung	(1) USB Typ A, vollständig konfigurierbar	(1) USB Typ A, vollständig konfigurierbar	(1) USB Typ A, vollständig konfigurierbar
ANSCHLÜSSE ZU DEN COMPUTERN			
Video-Eingang	(1) DVI-D 23-polig (Buchse)	(1) HDMI 1.4	(1) DisplayPort
Tastatur/Maus-Eingaben	(1) USB Typ-B	(1) USB Typ-B	(1) USB Typ-B
Audio-Ausgang	(1) Stereo 3,5-mm-Buchse	(1) Stereo 3,5-mm-Buchse	(1) Stereo 3,5-mm-Buchse
CAC-Unterstützung	(1) USB Typ B	(1) USB Typ B	(1) USB Typ B

BLACK BOX®

Warum Black Box?

Expertise

Die Projektingenieure von Black Box unterstützen Sie bei der Systembewertung, dem Design, der Implementierung und Schulung.

Angebotsbreite

Black Box bietet das umfassendste Angebot an technischen KVM-Lösungen in der Branche.

Support

Unser engagiertes Team hochqualifizierter Support-Techniker steht Ihnen das ganze Jahr über kostenlos telefonisch zur Verfügung und sorgt so für absolute Zufriedenheit.

Garantien

Unsere Secure KVM-Switches werden mit einer 3-Jahres-Garantie geliefert, Erweiterungsoptionen sind verfügbar.

Erfahrung

Black Box bietet seit 1976 führende Technologielösungen und unterstützt mehr als 175.000 Kunden in 150 Ländern beim Aufbau, der Verwaltung, Optimierung und Sicherung von IT-Infrastrukturen.

Kompetenzzentrum

Black Box bietet ein Center of Excellence mit professionellen Dienstleistungen und Support-Vereinbarungen, die dazu beitragen, die Systeme der Kunden zu optimieren und die Betriebszeit zu maximieren.

Service Level Agreements

Unsere Service Level Agreements bieten unseren Kunden Zugang zu technischem Support, Produktschulungen, engagierten Anwendungstechnikern und vielem mehr.

MEHR ERFAHREN BLACKBOX.COM/SECUREKVM