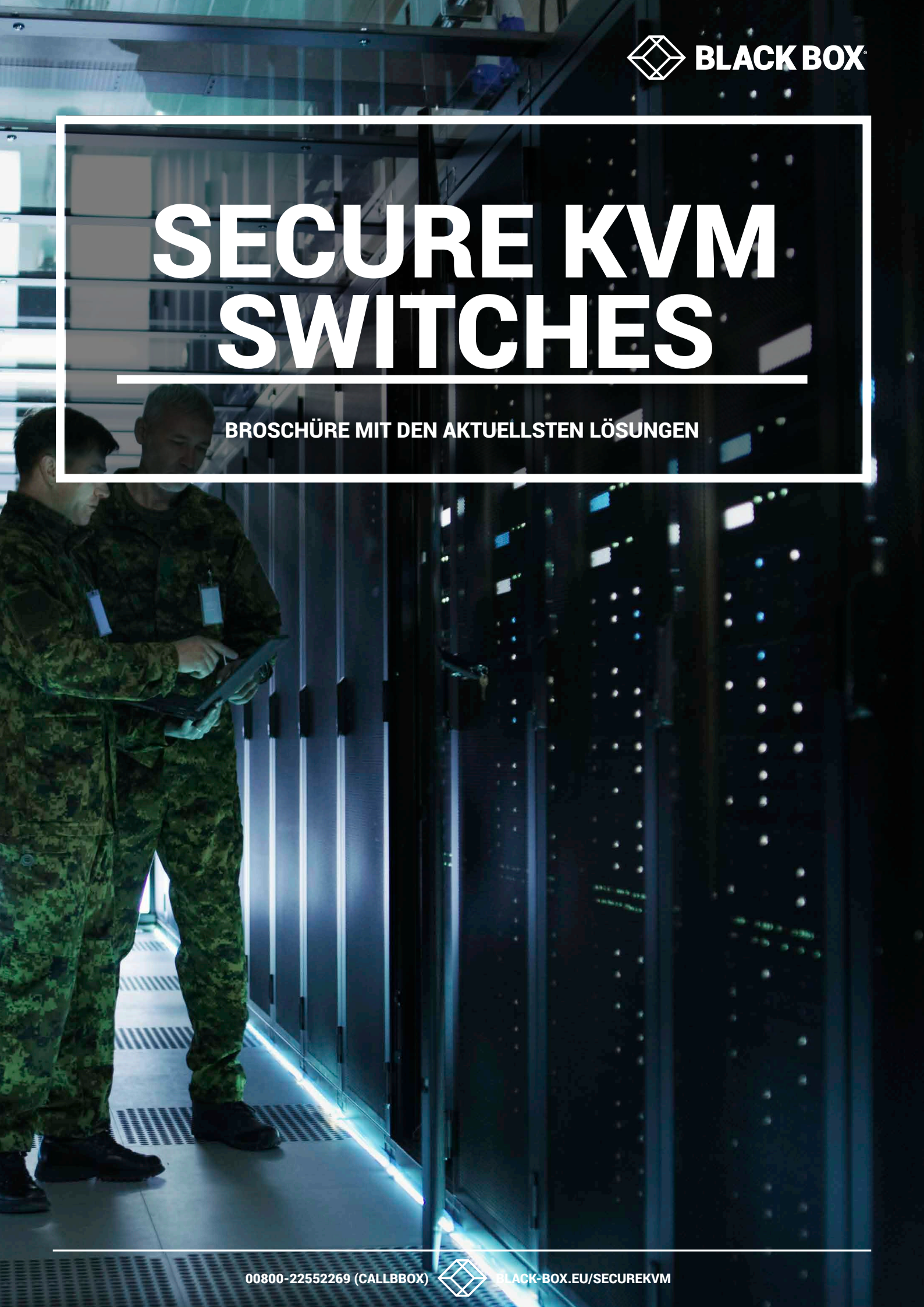


BLACK BOX

SECURE KVM SWITCHES

BROSCHÜRE MIT DEN AKTUELLSTEN LÖSUNGEN

BEKÄMPFEN SIE EINE VIELZAHL VON SICHERHEITSBEDROHUNGEN, DIE ENTSTEHEN, WENN EINE KONSOLE AN COMPUTERN MIT UNTERSCHIEDLICHEN SICHERHEITSSTUFEN GEMEINSAM GENUTZT WIRD

GRÜNDE FÜR SECURE KVM

Cyberbedrohungen entwickeln sich ständig weiter, nehmen zu und werden jeden Tag raffinierter. Unsere Abhängigkeit von Technologie, die gemeinsame Nutzung globaler Ressourcen und die Notwendigkeit der Zusammenarbeit in Echtzeit haben zu einem zunehmenden Web der Daten geführt. Auch wenn Interkonnektivität uns hilft, effizienter und effektiver zusammenzuarbeiten, macht sie uns anfälliger für verheerende Cyberangriffe.

Viele Verteidigungsbehörden und andere Organisationen nutzen fortschrittliche Sicherheitsmaßnahmen, um Netzwerke zu isolieren und Informationen vor Bedrohungen von außen zu schützen. Es gibt jedoch einen Ort, an dem isolierte Netzwerke und sensible Informationen zusammen kommen: am Desktop des Benutzers.

Traditonelle KVM Switches sind für Cyberangriff anfällig und können Cyberkriminellen den Zugriff auf klassifizierte Daten ermöglichen. Wenn ein Cyberkrimineller Informationen von einem klassifizierten Server stehlen möchte, kann er ein USB-Laufwerk mit Malware (Viren) in einen KVM-Switch stecken, um auf mehrere Server, statt nur auf einen, zuzugreifen. KVM-Switches sind außerdem für die böswillige Nutzung von LCD-Monitoren (über EDID-Signale), Mikrofonen oder unangemessene CAC-Implementierung anfällig.

Außerdem können Cyberkriminelle Hardwareinformationen über Schallwellen von traditionllen KVM Switches abfangen. Sie können programmierbare ROM-Sequenzen aus Schallwellen erhalten, mit denen Cyberkriminelle den Server neu konfigurieren oder programmieren können, um ihn unsicher zu machen. Durch diese Methoden können eine Unmenge klassifizierter Informationen in die falschen Hände gelangen und verwendet werden, um der Organisation zu schaden.

TRADITIONELLE KVM SWITCHES

KVM Switches ermöglichen den Zugriff und die Verwaltung mehrerer Computer von einer einzigen Anwenderkonsole mit einer Tastatur, einer Maus und einem Monitor. Benutzer können ganz einfach auf Informationen und Anwendungen auf komplett getrennten Systemen zugreifen, indem sie auf eine Befehl eingeben oder eine Taste drücken.

KVM-Technologie bietet Überwachungslösungen für Automatisierung, Prozesse und Workflow. Benutzer erhalten dadurch verbesserte Bedienbarkeit und eine schnellere Investitionsrendite aufgrund von mehr Ergonomie und Produktivität am Arbeitsplatz. KVM-Switches ermöglichen es Benutzern, Platz zu sparen, weil weniger Eingabegeräte genutzt werden, Kosten durch Beseitigung redundanter Peripheriegeräte zu sparen und in kritischen Situationen schneller zu reagieren.

SS4P-DH-DP-UCAC

SECURE KVM SWITCHES SORGEN DAFÜR, DASS SENSIBLE DATEN KLASSIFIZIERT BLEIBEN.

Ein Secure KVM Switch ist ein Desktop-Switch mit 2, 4, 8 oder 16 Ports, der Kontrolle aber auch die Isolierung der Rechner bietet, die mit Netzwerken mit unterschiedlichen Sicherheitsklassifizierungen verbunden sind. Anders als traditionelle KVM-Switches können Secure KVM Switches nur mithilfe von Drucktasten gesteuert werden. Hotkey-Befehle sind deaktiviert, was sicherstellt, dass nur die richtigen Benutzer Zugriff haben.

Secure KVM Switches erlauben einem USB-Laufwerk, das nicht erkannt wird, keinen Zugriff auf irgendwelche Informationen. Administratoren können auswählen, welche USB-Geräte autorisiert oder erkannt werden. Und sie verfügen über einen nicht neu programmierbaren ROM, um das Abfangen von Hardwareinformationen aus Schallwellen zu blockieren. Und das ist nur die Spitze des Eisbergs. Secure KVM Switches tun viel, viel mehr für den Schutz staatlicher Behörden und anderer Unternehmen vor den gefährlichsten Cyberbedrohungen.

Jetzt, wo Desktop-Sicherheit wichtiger als je zuvor ist, stellt Black Box eine neue Linie Secure KVM- und KM-Switches vor. NIAP 3.0-zertifizierte Secure KVM Switches bieten vollständige Isolation zwischen Computernetzwerken bei gleichzeitiger Nutzung desselben Satzes an Peripheriegeräten. Jeder Port verwendet seinen eigenen isolierten Datenkanal, um sicherzustellen, dass absolut keine Daten zwischen Ports mit klassifizierten Informationen und Ports mit nicht vertrauenswürdigen Systemen übertragen werden. Eine Vielzahl von Sicherheitsmerkmalen schützen vor Cyberangriffen, während das manipulationssichere Hardwaredesign physische Angriffe verhindert.

NIAP-SCHUTZPROFIL FÜR SECURE KVM

Bis vor kurzem verwendete die National Information Assurance Partnership (NIAP) das Common Criteria Evaluation & Validation Scheme (CCEVS) zur Bewertung und Zulassung von KVM-Switches für die Sicherheitsanwendungen.

Die NIAP hat das Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement für die Anwendung der Common Criteria implementiert und verwendet keine Evaluation Assurance Levels (EAL) für die Bewertung mehr.

Dies stärkt die Bewertung durch Fokussierung auf technologiespezifische Sicherheitsanforderungen.

Als Folge wurde das Protection Profile (PP) für Switches mit gemeinsamer Nutzung von Peripheriegeräten auf das PPS 3.0 NIAP Protection Profile for Peripheral Sharing Switch Version 3.0 aktualisiert, das aus Tests in Bezug auf den Prozess des Designs, der Prüfung, der Verifizierung und der Lieferung von Sicherheitsprodukten besteht. Dieses Schutzprofil ist ein internationaler, standardisierter Prozess für die Bewertung, Validierung und Zertifizierung der Sicherheit von Informationstechnologie.

STRIKTE SICHERHEITSMERKMALE IN SECURE KVM SWITCHES VON BLACK BOX

- Mechanische, elektrische und optische Signalisolierung zur Verhinderung von Hacking -> absolute Isolation und keine Datenlecks zwischen sicheren Ports und der Außenwelt
- Geschützte Firmware verhindert, dass Eindringlinge die Firmware neu programmieren oder lesen (nicht re- programmierbarer ROM).
- Optoisolierte USB-Ports und Löschen des Tastatur- und internen Cache sorgen dafür, dass USB-Datenpfade voneinander elektrisch isoliert sind, um USB-Datenlecks zwischen Ports zu verhindern.
- Sichere EDID-/Video- & Aux-Emulation schränkt die Erkennung neu verbundener Displays während Umschaltvorgängen ein. Dies verhindert, dass unerwünschte und ungesicherte Daten zwischen den Computern und dem Display übertragen werden.
- Gehäuse-Intrusionsschutz: mit aktiven, manipulationssicheren Schaltern und externen Hologramm-Verschlusssicherungen
- Optionale konfigurierbare Common Access Card (CAC)-Unterstützung für Smartcards, biometrische Leser und Registrierung externer USB-Geräte
- Unidirektionaler Datenfluss zu speziellen Peripheriegeräten wie einem Projektor, Drucker oder Audiosystem
- Gemäß NIAP PP 3.0 zertifiziert, der höchsten Common Criteria-Stufe (Protection Profile for Peripheral Sharing Switch Version 3.0)
- TAA-konform und in den USA hergestellt

GETESTET UND GEPRÜFT GEMÄSS DEM NEUESTEN NIAP PP 3.0-SICHERHEITSPROFIL

Secure KVM Switches von Black Box sind für die Verwendung in sicheren Verteidigungs- und Geheimdienstanwendungen gedacht, wenn sensible Daten geschützt werden müssen. Die Secure KVM Switches von Black Box sind NIAP PP 3.0-zertifiziert und mit den höchsten Sicherheitsmerkmalen ausgestattet, die die heutigen sicheren Kontrollstandards der Informationssicherheit erfüllen. Die Switches enthalten einzigartige Hardwarekonfigurationen, die Datenlecks zwischen PCs und angeschlossenen Peripheriegeräten verhindern und alle potenziellen Cyberbedrohungen beseitigen.

MEHRSTUFIGE SICHERHEIT FÜR STRENGE INFORMATIONSSICHERHEIT

Eine absolute Isolierung mechanischer, elektrischer und optischer Signale durch Air-Gapping verhindert Hacking-Angriffe und Datenlecks zwischen Anschlüssen und der Außenwelt. Jeder Anschluss des Secure KVM Switch verwendet seine eigenen, isolierten Datenkanäle. Beim Umschalten auf einem anderen Zielcomputer löscht der KVM-Switch erst den internen Cache und die Tastaturdaten, um sicherzustellen, dass sich keine Daten mehr im Kanal befinden. Die unveränderliche, sichere Firmware und der ROM sind nicht neu programmierbar. Dies verhindert, dass Eindringlinge Firmware lesen, entfernen oder unerwünschte Firmware-Upgrades neu programmieren.

GEHÄUSE-INTRUSIONSSCHUTZ.

Die Secure KVM Switches verfügen über manipulationssichere Schalter, externe Hologramm-Siegel und eine langlebige, manipulationssichere Batterie. Wenn die Abdeckung vom Gehäuse entfernt wird, schaltet der KVM Switch die Verbindung zu allen angeschlossenen PCs und Peripheriegeräten ab und deaktiviert alle Funktionen zum Schutz vor physischen Eindringversuchen.

TASTATUR- & MAUSEMULATION

Der Secure KVM Switch emuliert das Vorhandensein einer Tastatur und Maus für jeden über ein USB-Kabel angeschlossenen Computer. Sowohl ausgewählte als auch nicht ausgewählte Computer halten eine konstante Verbindung mit den Tastatur-/Mausemulationssteuerungen des Switch aufrecht, was ultraschnelle Umschaltung ermöglicht und die Erkennung neu verbundener Peripheriegeräte während Umschaltvorgängen einschränkt. Die Emulation von Tastatur und Maus verhindert außerdem eine direkte Verbindung zwischen Peripheriegeräten und den angeschlossenen Computern, sodass Systeme vor potenziellen Schwachstellen geschützt sind.

VOLLSTÄNDIG KONFIGURIERBARER COMMON ACCESS CARD (CAC)-PORT FÜR EXTERNE USB-PERIPHERIEGERÄTE

Viele Secure KVM Switches unterstützen CAC (Common Access Card)-Geräte wie Smartcard- und biometrische Leser, was die Sicherheit bei Verwendung des Geräts erhöht. Black Box geht bei der CAC-Sicherheit jedoch noch weiter und ermöglicht authentifizierten Administratoren die Registrierung und Zuweisung spezifischer Peripheriegeräte am CAC-Port (optional). Benutzer können dann die Verbindung zwischen dem zugewiesenen Gerät neben der KVM-Umschaltung der verbundenen Computer umschalten.

EINSCHRÄNKUNG NEUER MONITORVERBINDUNGEN WÄHREND DER UMSCHALTUNG

Die Secure KVM Switches simulieren immer ein generisches EDID, was den Betrieb der meisten angeschlossenen Monitore erlaubt. Ausgewählte als auch nicht ausgewählte Computer halten eine konstante Verbindung mit den Video- und AUX-Emulationssteuerungen des Switch aufrecht, was ultraschnelle Umschaltung ermöglicht und die Erkennung neu verbundener Monitore während Umschaltvorgängen einschränkt. Dadurch wird das System vor potenziellen Schwachstellen durch unerwünschte und unsichere Datenübertragung über DDC-Leitungen geschützt.

IDEAL FÜR VIELE BRANCHEN

REGIERUNG

VERTEIDIGUNG & MILITÄR

KONTROLLRÄUME FÜR DAS VERKEHRSMANAGEMENT

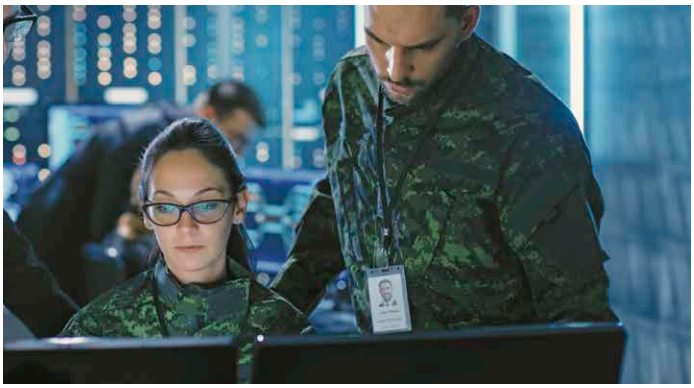
BANKEN UND FINANZWESEN

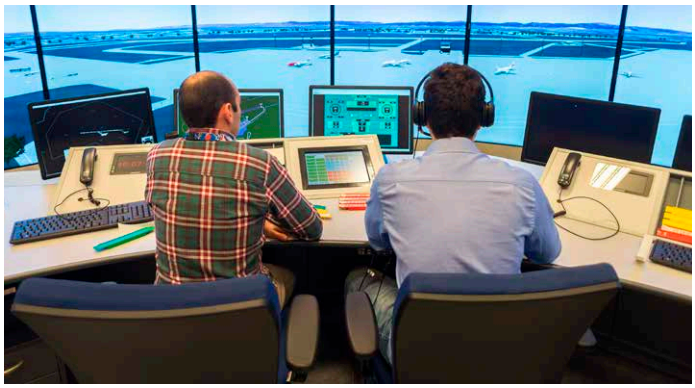
BILDUNGSWESEN

GESUNDHEITSWESEN

ENTWICKLUNGS- & FORSCHUNGSABTEILUNGEN

ANWENDUNGSFÄLLE





KOMMUNIKATIONSZENTRUM IM VERTEIDIGUNGSSEKTOR

Ein Kunde aus der Verteidigung kam mit zwei dringlichen Problemen zu Black Box: ineffizienter Netzwerkzugriff und ineffizienter Arbeitsplatz.
Seine Bediener benötigten Zugriff auf mehrere Computer-netzwerke in sicheren Kommunikationszentren. Dies war ein zeitaufwändiger Prozess, da für jedes Computernetzwerk eine eigene Tastatur, ein eigener Monitor und eine eigene Maus erforderlich waren. Die Bediener mussten den Schreibtisch wechseln, um auf die unterschiedlichen Systeme mit sensiblen, offenen und geheimen Daten zuzugreifen. Dafür waren sechs verschiedene Monitore, sechs verschiedene Tastaturen und sechs verschiedene Mäusen nötig, was den Arbeitsbereich unordentlich und unübersichtlich machte.
Um diese Probleme zu bewältigen, kauften sie 8-Port Secure KVM Switches von Black Box, die die Konfiguration auf einen Monitor, eine Tastatur und eine Maus verringerte, aber sicheren Zugriff auf alle Systeme erlaubt. Die Bediener, die zwischen mehreren Netzwerken wechseln, sparen wertvolle Zeit und durch weniger Schreibtische gibt es mehr Platz im engen Büro. Sie arbeiten jetzt an einem ergonischem Arbeitsplatz viel effizienter, während gleichzeitig sichergestellt ist, dass ihre lebenswichtigen Daten nicht gefährdet sind.

LUFTFAHRT

Ein Unternehmen kontaktierte Black Box, da es eine äußerst sichere Lösung für ein Luftfahrtprojekt benötigte. Projektingenieure mussten zwischen einem offenen (grünen) und sicheren (roten) Netzwerk umschalten. Black Box schlug den Secure KVM Switch mit vier DVI USB-Ports vor, der alle ihre Anforderungen perfekt erfüllt. Inzwischen wurden bereits über 1.000 Secure KVM Switches installiert.

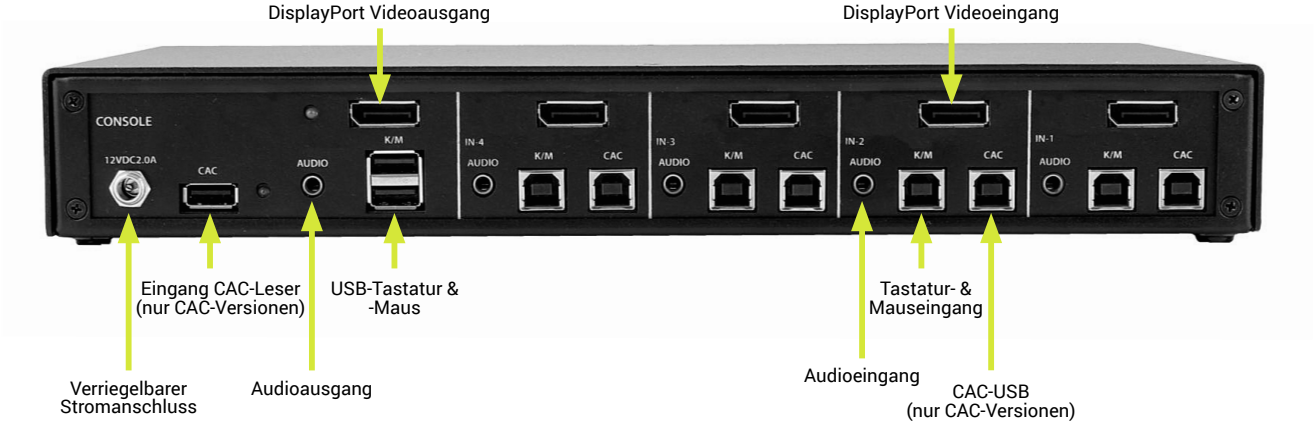
UNTERNEHMEN MIT ZAHLUNGS-UND KUNDENDATEN

Die gemeinsame Nutzung globaler Ressourcen und die Notwendigkeit einer Zusammenarbeit in Echtzeit haben zu einem zunehmenden Web der Daten geführt. Auch wenn Interkonnektivität Organisationen hilft, effizienter und effektiver zusammenzuarbeiten, macht sie sie anfälliger für verheerende Cyberangriffe. Letztendlich müssen Systeme mit Internetzugriff von anderen Systemen getrennt gehalten werden, die für sensible Unternehmens- oder persönliche Daten verwendet werden. Zur Aufrechterhaltung ihrer Informationssicherheit ersetzen viele Organisationen traditionelle durch Secure KVM Switches.

SECURE KVM – PRODUKTÜBERBLICK

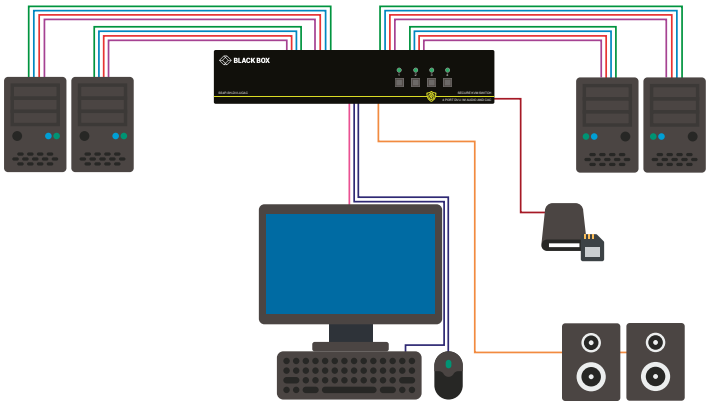
DESIGN DER SECURE KVM SWITCHES

Beispiel eines Secure KVM Switch mit 4 Ports für einen Benutzer mit DisplayPort, USB und CAC (SS4P-SH-DP-UCAC)



ARTEN VON SECURE DESKTOP KVM SWITCHES

SECURE DESKTOP-KVM-SWITCHES FÜR EINEN BENUTZER

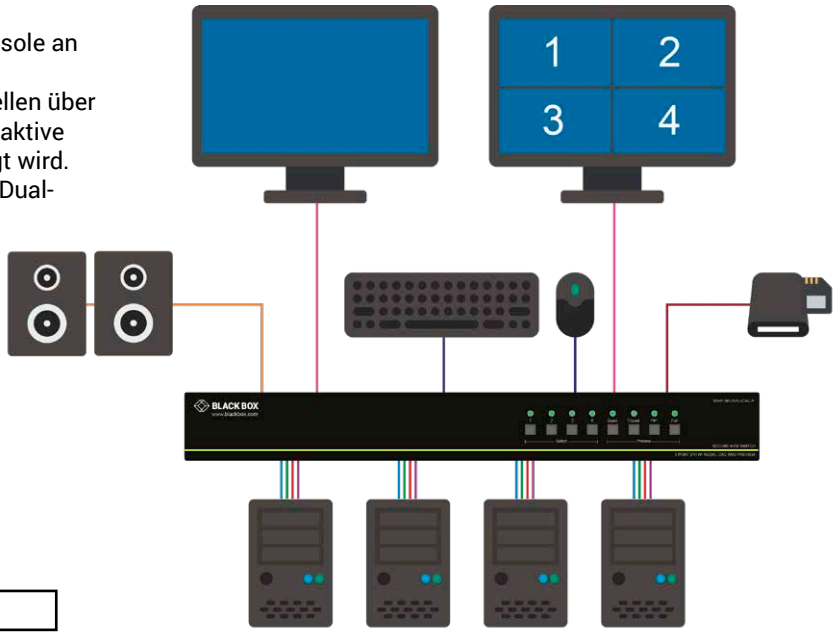


- Gemeinsame Nutzung einer einzigen Benutzerkonsole an zwei, vier, acht oder 16 Computern
- Erhältlich mit DVI-I-, DisplayPort- oder HDMI-Video
- Hochwertiges DisplayPort 1.2- oder HDMI-Video mit Auflösungen bis zu 4K Ultra-HD (3840 × 2160 bei 30 Hz) und bester DVI-I Dual-Link-Auflösung bis zu 2560 x 1600 bei 60 Hz
- Varianten für Konsolen mit einem, zwei oder vier Monitoren
- USB-Tastatur/-Maus plus Stereoton
- Erhältlich mit oder ohne CAC-Unterstützung
- NIAP 3.0-zertifiziert

i Detaillierte Produktübersicht auf den Seiten 9 & 10.

SECURE DVI-I KVM-SWITCH FÜR EINEN BENUTZER MIT 4-IN-1-ANZEIGE AM BILDSCHIRM

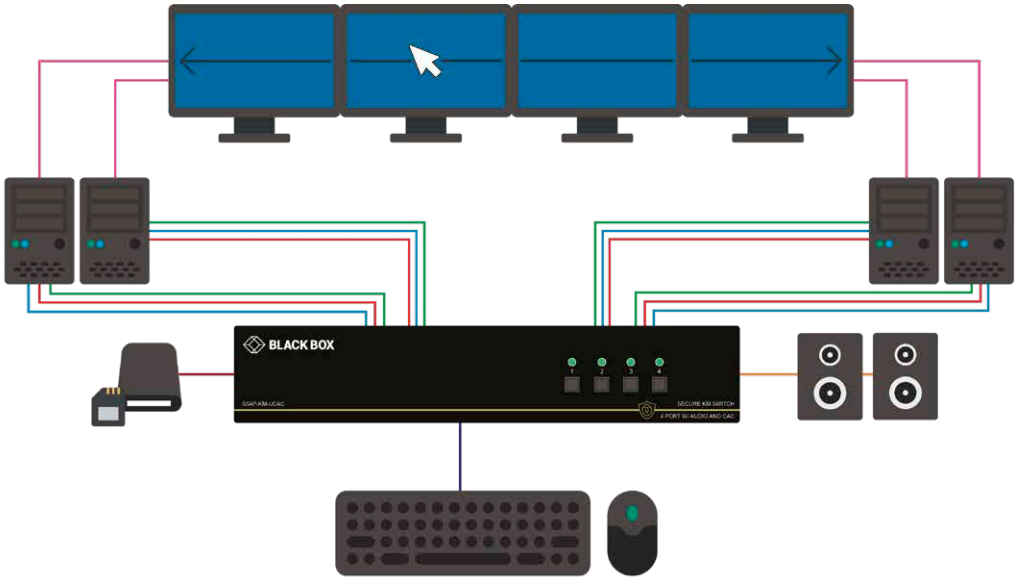
- Gemeinsame Nutzung einer einzigen Benutzerkonsole an vier Computern
- Gleichzeitige Anzeige und Überwachung aller Quellen über 4-in-1-Anzeige auf einem Bildschirm, während der aktive Rechner auf einem zweiten Vollbild-Display gezeigt wird.
- DVI-I-Video mit Unterstützung für Single-Link DVI, Dual-Link DVI und VGA
- Beste Auflösung bis 2560 x 1600 (Dual Link DVI)
- USB-Tastatur/-Maus plus Stereoton
- CAC-Unterstützung für Smartcard-Leser und spezielle Peripheriegeräte-Zuweisung
- NIAP 3.0-zertifiziert



i Detaillierte Produktübersicht auf Seite 10.

SECURE DESKTOP KM SWITCHES (GLIDE & SWITCH)

- Umschalten durch Bewegen der Maus von Monitor zu Monitor (Glide & Switch)
- Gleichzeitiges Anzeigen allen Quellen: Monitore sind weiterhin direkt mit dem Rechnern verbunden
- Gleichzeitige Nutzung einer einzigen Benutzerkonsole mit USB-Tastatur und -Maus an vier oder acht Computern
- Stereoton-Unterstützung
- Erhältlich mit oder ohne CAC-Unterstützung
- NIAP 3.0-zertifiziert

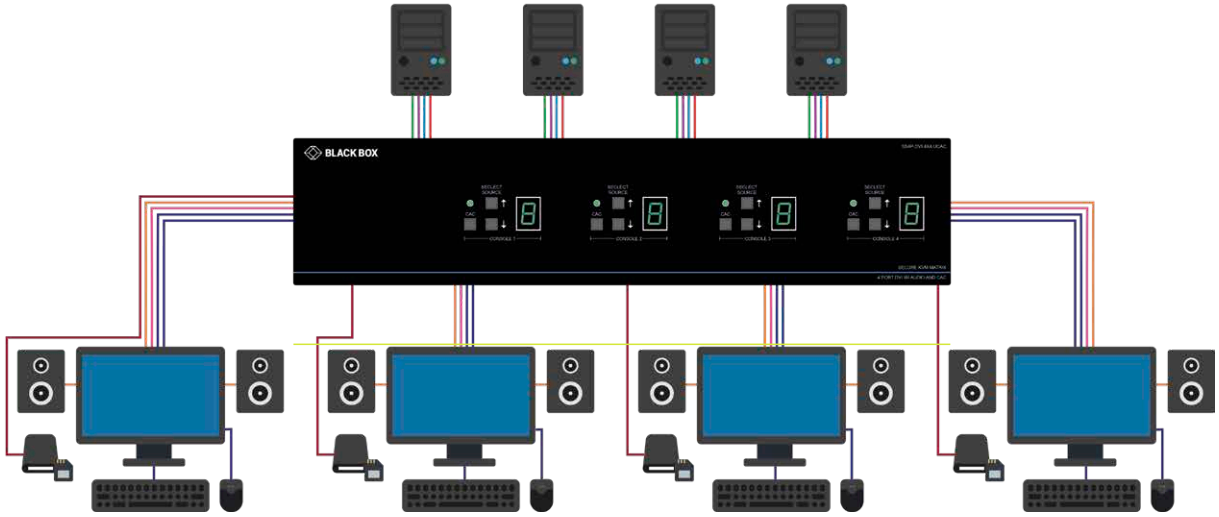


i Detaillierte Produktübersicht auf Seite 11

SECURE KVM – PRODUKTÜBERBLICK

SECURE DVI-I KVM-MATRIX-SWITCHES FÜR MEHRERE BENUTZER

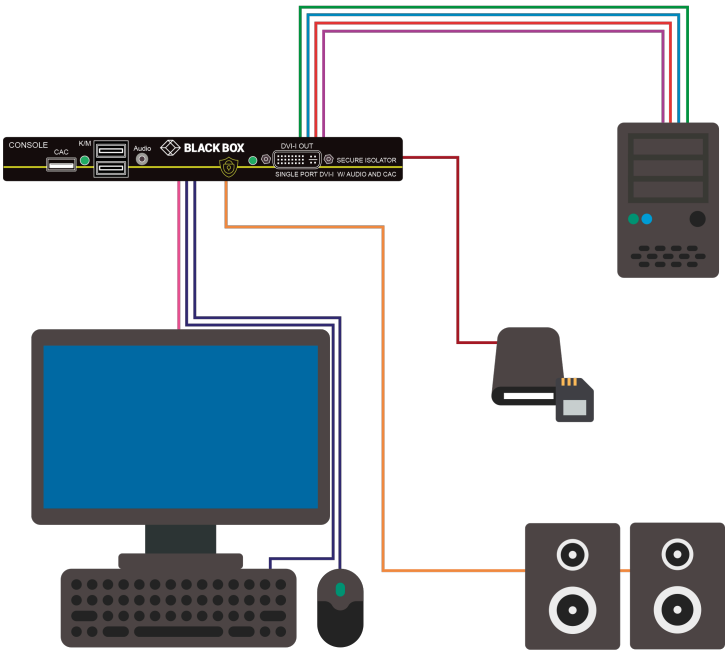
- Zugriff für zwei oder vier Benutzer auf vier oder acht Computer
- DVI-I-Video mit Unterstützung für Single-Link DVI, Dual-Link DVI und VGA bis zu 2560 x 1600
- USB-Tastatur/-Maus plus Stereoton
- CAC-Unterstützung für Smartcard-Leser und spezielle Peripheriegeräte-Zuweisung
- Unterstützung der meisten Monitore über sicheres EDID-Lernen/Emulation
- Windows-, Mac- und Linux OS-kompatibel
- NIAP 3.0-zertifiziert



i Detaillierte Produktübersicht auf Seite 11

SECURE KVM PROTEKTOR

- Blockiert die direkte Verbindung zwischen einem Host-PC oder Laptop und einem Peripheriegerät, das Sicherheitsbedrohungen ausgesetzt ist, wie zum Beispiel einem Drucker, einem Projektor, einem Lautsprecher oder irgendeinem anderen Peripheriegerät mit Zugriff auf einen klassifizierten Computer oder ein klassifiziertes Netzwerk.
- Stellt unidirektionalen Datenfluss von Video, USB und Audio vom Host-PC zum Peripheriegerät sicher.
- Anschlüsse für DVI-I-Video, USB und Audio
- Unterstützung der meisten Monitore über sicheres EDID-Lernen/Emulation
- Stereoton-Unterstützung
- Windows-, Mac- und Linux OS-kompatibel
- CAC-Unterstützung
- NIAP 3.0-zertifiziert



i Detaillierte Produktübersicht auf Seite 10

4K DISPLAYPORT SECURE KVM SWITCHES, NIAP 3.0-ZERTIFIZIERT

						
Artikelnummer	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
Beschreibung	2-Port Secure KVM Switch für einen Benutzer, 4K DisplayPort Single-Head	4-Port Secure KVM Switch für einen Benutzer, 4K DisplayPort Single-Head	8-Port Secure KVM Switch für einen Benutzer, 4K DisplayPort Single-Head	2-Port Secure KVM Switch für einen Benutzer, 4K DisplayPort Dual-Head	4-Port Secure KVM Switch für einen Benutzer, 4K DisplayPort Dual-Head	4-PortSecure KVM Switch für einen Benutzer, 4K DisplayPort Quad-Head
Anzahl der Quellen (max.)	2	4	8	2	4	4
Computerkompatibilität	Windows, Mac und Linux OS					
Max. Auflösung	4K bis zu 3840 x 2160 bei 30 Hz					
Monitorkompatibilität	Die meisten Monitore über sicheres EDID-Lernen/Emulation					
ANSCHLÜSSE ZUR BENUTZERKONSOLE						
Monitoranschlüsse	1x DisplayPort 1.2			2x DisplayPort 1.2		4x DisplayPort 1.2
Tastatur-/ Mausanschlüsse	2x USB 1.1 Typ A, nur Tastatur und Maus					
Audioausgang	1x 3,5mm-Audiobuchse mit Balanced-Lautsprecherausgängen und Umschaltung.					
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ A, vollständig konfigurierbar					
COMPUTERPORTS						
Videoeingänge	1x DisplayPort 1.2 pro Quelle			2x DisplayPort 1.2 pro Quelle		4x DisplayPort 1.2 pro Quelle
Tastatur-/Mauseingang	1x USB 1.1 Typ B pro Quelle mit USB-Emulation					
Audioeingang	1x 3,5mm-Audiobuchse pro Quelle					
CAC-Unterstützung (nur UCAC-Modelle)	1 USB Typ B pro Quelle					

4K HDMI SECURE KVM SWITCHES, NIAP 3.0-ZERTIFIZIERT

				
Artikelnummer	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
Beschreibung	2-Port Secure KVM Switch für einen Benutzer, 4K HDMI Single-Head	4-Port Secure KVM Switch für einen Benutzer, 4K HDMI Single-Head	2-Port Secure KVM Switch für einen Benutzer, 4K HDMI Dual-Head	4-Port Secure KVM Switch für einen Benutzer, 4K HDMI Dual-Head
Anzahl der Quellen (max.)	2	4	2	4
Computerkompatibilität	Windows, Mac und Linux OS			
Max. Auflösung	4K bis zu 3840 x 2160 bei 30 Hz			
Monitorkompatibilität	Die meisten Monitore über sicheres EDID-Lernen/Emulation			
ANSCHLÜSSE ZUR BENUTZERKONSOLE				
Monitoranschlüsse	1x HDMI 1.4		2x HDMI 1.4	
Tastatur-/Mausanschlüsse	2x USB 1.1 Typ A, nur Tastatur und Maus			
Audioausgang	1x 3,5mm-Audiobuchse mit Balanced-Lautsprecherausgängen und Umschaltung.			
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ A, vollständig konfigurierbar			
COMPUTERPORTS				
Videoeingänge	1x HDMI 1.4 pro Quelle		2x HDMI 1.4 pro Quelle	
Tastatur-/Mausanschlüsse	1x USB 1.1 Typ B pro Quelle mit USB-Emulation			
Audioeingang	1x 3,5-mm-Audiobuchse pro Quelle			
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ B pro Quelle			

DVI-I SECURE KVM-SWITCHES (VGA ÜBER ADAPTER), NIAP 3.0-ZERTIFIZIERT								
								
Artikelnummer.	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
Beschreibung	2-Port Secure KVM Switch für einen Benutzer, DVI-I Single-Head	4-Port Secure KVM Switch für einen Benutzer, DVI-I Single-Head	8-Port Secure KVM Switch für einen Benutzer, DVI-I Single-Head	16-Port Secure KVM Switch für einen Benutzer, DVI-I Single-Head	2-Port Secure KVM Switch für einen Benutzer, DVI-I Dual-Head	4-Port Secure KVM Switch für einen Benutzer, DVI-I Dual-Head	8-Port Secure KVM Switch für einen Benutzer, DVI-I Dual-Head	4-Port Secure KVM Switch für einen Benutzer, DVI-I Quad-Head
Anzahl der Quellen (max.)	2	4	8	16	2	4	8	4
Kompatibilität BS	Windows, Mac und Linux OS							
Max. Auflösung	2560 x 1600 bei 60 Hz							
Kompatibilität Monitor	Die meisten Monitore über sicheres EDID-Lernen/Emulation							
ANSCHLÜSSE ZUR BENUTZERKONSOLE								
Videoanschlüsse	1x DVI-I				2x DVI-I			4x DVI-I
Tastatur-/ Mausanschlüsse	2x USB 1.1 Typ A, nur Tastatur und Maus							
Audioausgang	1x 3,5mm-Audiobuchse mit Balanced-Lautsprecherausgängen und Umschaltung.							
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ A, vollständig konfigurierbar							
COMPUTERPORTS								
Videoeingänge	1x DVI-I pro Quelle				2x DVI-I pro Quelle			4x DVI-I pro Quelle
Tastatur/Maus	1x USB 1.1 Typ B pro Quelle mit USB-Emulation							
Audioeingang	1x 3,5mm-Audiobuchse pro Quelle mit Balanced-Lautsprecherausgängen und Umschaltung							
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ B pro Quelle							

	DVI-I MULTIVIEWER NIAP, NIAP 3.0-ZERTIFIZIERT	KVM PROTEKTOR, NIAP 3.0
		
Artikelnummer.	SS4P-SH-DVI-UCAC-P	SS1P-DVI-UCAC-P
Beschreibung	4-Port Secure KVM Switch, DVI-I mit 4-in-1-Multiview	1-Port Secure KVM Protektor
Anzahl der Quellen (max.)	4	Ein Peripheriegerät
Monitoranschlüsse zur Konsole	2	1
Max. Auflösung	2560 x 1600 bei 60 Hz	2560 x 1600 bei 60 Hz
ANSCHLÜSSE ZUR BENUTZERKONSOLE		ANSCHLÜSSE ZUM ERIPHERIEGERÄT:
Monitoranschlüsse	2 DVI-I (1x Vollbild, 1x Ansicht von vier Quellen)	1x DVI-I
Tastatur-/Mausanschlüsse	1x USB 1.1 Typ A	1x USB 1.1 Typ A
Audioausgang	1x 3,5mm-Audiobuchse	1x 3,5mm-Audiobuchse
CAC-Unterstützung	1x USB-Typ A, konfigurierbar	1x USB-Typ A, konfigurierbar
COMPUTERPORTS		
Videoeingänge	1x DVI-I pro Quelle	1x DVI-I
Tastatur-/Mausanschlüsse	1x USB 1.1 Typ B pro Quelle, emuliert	1x USB 1.1 Typ B emuliert
Audioeingang	1x 3,5mm-Audiobuchse pro Quelle	1x 3,5mm-Audiobuchse
CAC-Unterstützung - nur UCAC-Modelle	1x USB Typ B pro Quelle	1x USB Typ B

	DVI-I SECURE KVM-MATRIX-SWITCHES, NIAP 3.0-ZERTIFIZIERT				KM-SWITCHES, NIAP 3.0 GLIDE & SWITCH	
						
Artikelnummer.	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
Beschreibung	4x2 Secure KVM Matrix Switch, DVI-I	8x2 Secure KVM Matrix Switch, DVI-I	4x4 Secure KVM Matrix Switch, DVI-I	8x4 Secure KVM Matrix Switch, DVI-I	4-Port Secure KM-Switch	8-Port Secure KM-Switch
Anzahl der Quellen (max.)	4	8	4	8	4	8
Computerkompatibilität	Computer mit Windows, Mac und Linux OS				Windows, Mac und Linux OS	
Anzahl der Benutzer	2	2	4	4	1	1
Monitor an der Konsole	1	1	1	1	direkte Monitor/PC-Verbindung	
Max. Auflösung	2560 x 1600 bei 60 Hz				_	
Monitorkompatibilität	Die meisten Monitore über sicheres EDID-Lernen/Emulation				_	
ANSCHLÜSSE ZUR BENUTZERKONSOLE						
Monitoranschluss	1x DVI-I pro Konsole				keine, Monitore behalten direkten Computeranschluss	
Tastatur-/ Mausanschlüsse	2x USB 1.1 Typ A pro Konsole, nur Tastatur und Maus				2x USB 1.1 Typ A, nur Tastatur und Maus	
Audioausgang	1x 3,5-mm-Audiobuchse pro Konsole mit Balanced-Lautsprecherausgängen und Umschaltung				1x 3,5mm-Audiobuchse mit Balanced-Ausgang und Umschaltung.	
CAC-Unterstützung	1x USB Typ A pro Konsole, vollständig konfigurierbar				1x USB Typ A, vollständig konfigurierbar	
COMPUTERPORTS						
Videoeingänge	1x DVI-I pro Quelle				keine	
Tastatur-/ Mausanschlüsse	1x USB 1.1 Typ B pro Quelle mit USB-Emulation				1x USB 1.1 Typ B pro Quelle mit USB-Emulation	
Audioeingang	1x 3,5-mm-Audiobuchse pro Quelle mit Balanced-Lautsprecherausgängen und Umschaltung				1x 3,5mm-Audiobuchse pro Quelle	
CAC-Unterstützung (nur UCAC-Modelle)	1x USB Typ B pro Quelle				1x USB Typ B pro Quelle	

ZUBEHÖR	
Kabel für Secure KVM Switches	
SKVMCBL-DP-06	DisplayPort, USB, 3,5mm Audio; 1,8 m
SKVMCBL-HDMI-06	HDMI, USB, 3,5mm Audio; 1,8 m
SKVMCBL-DVI-06	DVI, USB, 3,5mm Audio; 1,8 m

KONTAKT MIT BLACK BOX

Wissen Sie nicht genau, was das Richtige ist? Kontaktieren Sie unsere KVM-Experten. Rufen Sie unter **00800-2255 2269** an oder besuchen Sie **WWW.BLACK-BOX.EU/TSC**.

DARUM SOLLTEN SIE SICH FÜR BLACK BOX ENTSCHEIDEN

KNOW-HOW
Die Projektingenieure von Black Box unterstützen Sie bei Systembewertung, Entwicklung, Implementierung und Schulung.

UMFANG DES PRODUKTANGEBOTS
Black Box bietet das umfangreichste Portfolio an KVM-Lösungen mit Support an.

SUPPORT
Um unserer Verpflichtung für eine vollkommene Kundenzufriedenheit nachzukommen, steht Ihnen unser engagiertes Team aus ausgezeichnet ausgebildeten Support-Technikern gerne und kostenlos zur Verfügung.

GEWÄHRLEISTUNGEN
Secure KVM Switches werden mit einer 3-jährigen Garantie geliefert; Verlängerungsoptionen sind verfügbar.

STARKE FINANZIELLE POSITION
Ein Jahresumsatz von fast als 1 Mrd. US-Dollar; börsennotiert (BBOX).

ERFAHRUNG
Durch die Lieferung von führenden Technologielösungen seit 1976 hilft Black Box über 175.000 Kunden in 150 Ländern beim Bauen, Verwalten, Optimieren und Sichern ihrer IT-Infrastruktur.

KOMPETENZZENTRUM
Black Box bietet ein Kompetenzzentrum mit professionellen Services und Supportverträgen, die Ihnen helfen, Systeme von Kunden zu optimieren und die Betriebszeit zu maximieren.

SERVICE LEVEL AGREEMENTS
Durch unsere Service Level Agreements erhalten unsere Kunden Zugang zu unserem technischen Support, zu Produktschulungen, zu dedizierten Anwendungsingenieuren und zu vielem mehr.