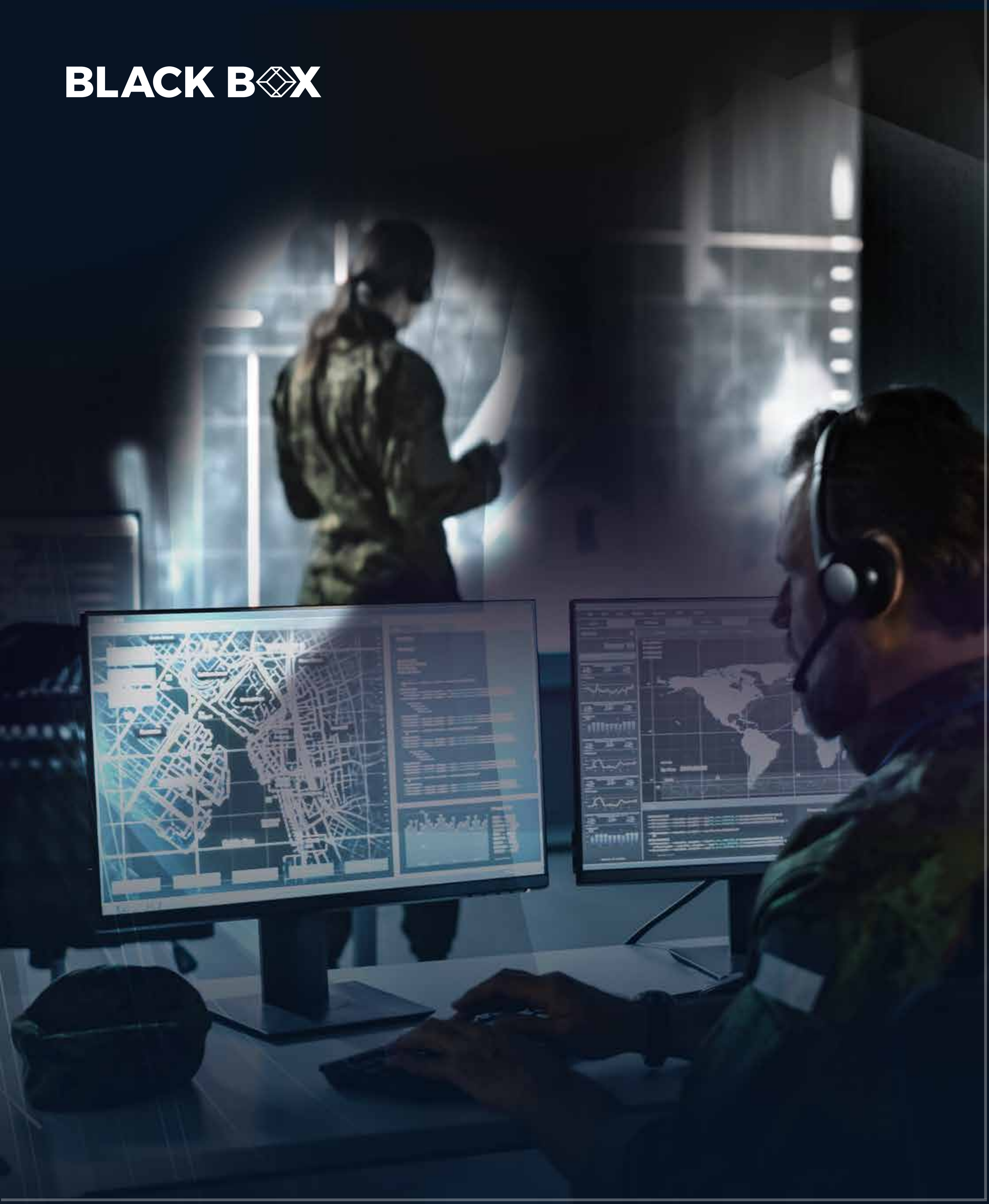


Meeting Cybersecurity Threats With Secure KVM Switches

The Impact and Importance of the New **NIAP Protection Profile V4.0**

Whether instigated within an organization or by an external person or group, cyber threats are growing more common and complex with each passing day. Massive high-profile cybersecurity breaches such as the Solar Winds supply chain attack in 2020 have brought organizations worldwide a greater sense of urgency in protecting against cyber threats. The COVID-19 pandemic has likewise driven increased concern over cyber threats, with information security being a top priority for businesses in terms of technology objectives*.

The very interconnectivity that today enables efficient, collaborative work in various organizations also presents vulnerabilities to potentially devastating cyber threats. Defense agencies and organizations across banking, finance, transportation, healthcare, and other sectors rely on advanced security measures to isolate their networks and safeguard information from outside threats. But to prevent classified or otherwise sensitive information from getting into the wrong hands, they also must address internal threats at the convergence of their networks and sensitive information: the operator console.

The connection of computer peripherals such as the keyboard and mouse to a computer or server introduces potential data leakage and hacking risks.

Internal threats range from unintended microprocessor malfunction and unexpected software bugs to malicious modification of software and use of crosstalk and timing analysis to identify signals and data flow patterns. Secure KVM (keyboard, video, mouse) switches are essential to fending off such threats. In addition to blocking data leakage between multiple connected computers/ servers, a secure KVM switch can prevent eavesdropping through LCD monitors (EDID signal exchange), microphones, or common access card (CAC) devices.

Built with true data-path isolation between systems and networks to ensure no data is leaked between secure ports and the outside world, secure KVM devices are the hidden champions in providing an essential layer of internal protection.

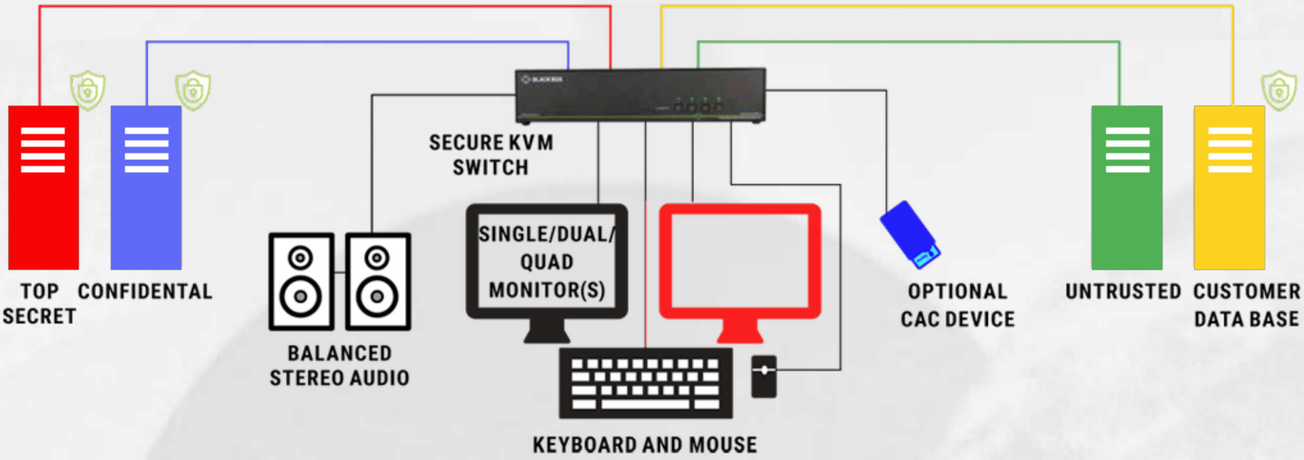
BLACK BOX

The Secure KVM Advantage

Typically deployed at the desktop, a secure KVM switch provides control and separation of multiple computers connected to networks of differing security classifications. Unlike traditional KVM switches, sophisticated secure KVM switches boast a variety of features designed to offer enhanced protection against data leakage and other threats. Rather than rely on software coding that can be manipulated, they build on physical features that are much harder to overcome. Absolute isolation of the mechanical, electrical, and optical signals prevents hacking and data leakage between the switch ports and the outside world.

Because the secure KVM switch emulates the presence of a keyboard and mouse for every attached computer through a USB cable, it eliminates the direct connection that could present potential vulnerabilities. The switch's video and AUX emulation controllers restrict discovery of newly connected monitors and shield the system from potential vulnerabilities through unwanted and unsecure data transmittance through DDC lines. Limited physical access and safeguards against any attempt at physical intrusion help to ensure that only authorized users have access and control.

Together, these features and capabilities enable a secure KVM switch to address the requirements of the most demanding applications, including deployment in government and military environments.



LEARN MORE BLACKBOX.COM/SECUREKVM

Certifying Secure KVM via NIAP Evaluation

The National Information Assurance Partnership (NIAP) is responsible for U.S. implementation of the Common Criteria (CC). NIAP manages a national program for developing Protection Profiles (PP), evaluation methodologies, and policies that will ensure achievable, repeatable, and testable requirements. In partnership with the National Institute of Standards and Technology (NIST), NIAP also approves Common Criteria Testing Laboratories to conduct these security evaluations in private sector operations across the U.S, which is the global driving force for the widest available mutual recognition of secure IT products.

NIAP is a technical community of cybersecurity specialists from government, military, equipment vendors, and official testing laboratories, which together create PPs based on essential safety requirements (ESR), handed down from within government, for a specific technology type. These NIAP PPs define the most basic security posture that the government will expect of a product of that technology type when it comes into their environment.

To ensure that they introduce no additional risk when being deployed in the national security sector, secure KVM switches are evaluated according to a NIAP PP that describes security requirements for a Peripheral Sharing Switch (PSS) connecting a common set of peripherals to one or more attached computers.

The NIAP PP for secure desktop KVM provides a baseline set of requirements intended to mitigate well-defined and well-described threats. Requirements and test scopes for secure KVM switches are high and include, for example, type, usage, and authorization of connected peripherals (monitor, keyboard, mouse, other USB devices); data flow and anti-tamper rules; audio/data/channel

isolation; CAC settings; and video protocol authorization and handling.

Successful evaluation of a secure KVM switch by an authorized Common Criteria Testing

Laboratory validates that a specific product meets security requirements for U.S. national security system procurement. Certification for the latest NIAP PP therefore simplifies product selection by government procurers, as well by as integrators and end users in other markets.

The Shift From NIAP PP PSD V3.0 to NIAP PP PSD V4.0

Because cybersecurity threats evolve over time, so too does the protection profile to ensure certified products do not add risk to the deployed environment. For this reason, NIAP recently introduced NIAP PP PSD V4.0 as the current profile for technologies including secure KVM switches. Established as the official current protection profile on Jan. 18, 2020, NIAP PP PSD V4.0 addresses upgrades and updates to the government's security posture since NIAP PP PSD V3.0 was first published more than six years ago on February 13th, 2015.

NIAP PP PSD V4.0 takes into account all of the technical and iterative decisions made to government requirements for KVM switches over those years. In addition to allowing for new interfaces, the new protection profile identifies other interfaces that are not allowed.

While many details of NIAP PP 4.0 differ from 3.0, a half-dozen of these updates are notable for vendors and end users. These key changes include the following:

- More specific testing for video sub-protocols. Products claiming different video interfaces, such as HDMI or DVI, are tested against different protocols specific to those interfaces.
- More stringent testing for audio isolation.

- Modular design of the protection profile so that vendors need only claim the peripherals their devices actually use.
- Restriction against a target of evaluation (TOE) having any unapproved external interfaces. It is no longer allowable to indicate that a PS/2 port is present on the TOE and is just outside the evaluation scope.
- Restriction against certification of a matrix TOE.
- A physical tamper response is now optional rather than mandatory.

Many of the requirements in NIAP PP PSD V4.0 are similar to those in 3.0 but have been renamed and substantially reorganized to permit more granular testing. NIAP is undertaking a similar process with all PPs, modularizing elements so that evaluation can focus more specifically on applicable requirements. This change also helps to ensure that Security Functional Requirements (SFR) include fewer if/then statements.

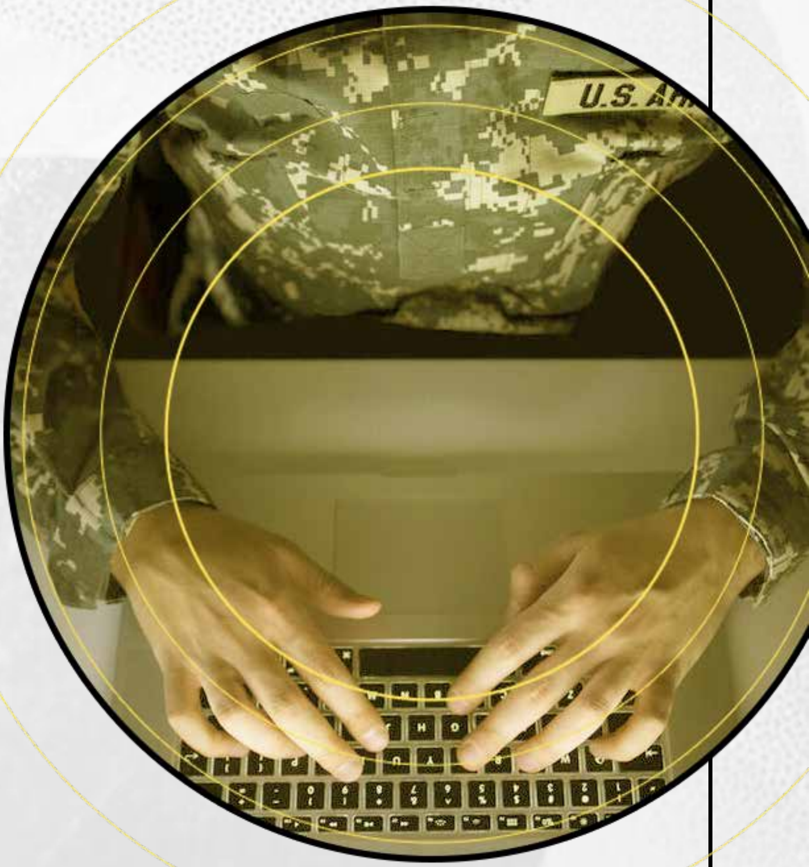
NIAP TAA COMPLIANT Common Criteria

BLACK BOX

Quick Technology Overview
NIAP PP PSD V3.0 vs NIAP PP PSD V4.0

{.PSD 4.0}	{.PSD 4.0}
One single protection profile for all switch types	Base-protection profile with individual modules so that only requirements for relevant peripheral types are claimed
Ambiguity on types of devices that are or aren't permitted	More explicit guidance on allowed/prohibited device types (e.g. matrix devices no longer allowed)
Isolation requirements integrated with Security Target	Isolation materials may be ST addendum or separate document
Tests with large numbers of conditional steps based on product functionality	Granular requirements align specifically with test activities so that it's more clear from claimed requirements what specific tests were done
All models of a product family on a single Security Target	Different Security Targets for different supported peripherals (e.g. CAC and non-CAC models are different 'configurations'
Generic testing for video protocols	Specific list of allowed and rejected sub-protocols based on the supported video protocols (DP, DVI, HDMI, USB-C, VGA)
Mandatory tamper response requirements	Tamper response is optional because some devices may have swappable cards for different peripheral types (in which case tamper seals are sufficient)
No audio in (microphone) capability	Audio in is permitted but only if no other peripheral types are supported by the device (i.e. microphone cannot coexist with speakers)
PS/2 ports allowed	PS/2 ports prohibited
No specific multi-viewer requirements	Multi-viewers are permitted but must use OSD to identify the active video channel(s)

Why Shift to NIAP PP PSD V4.0



While it's quite possible that a product certified for NIAP PP PSD V3.0 can also earn NIAP PP PSD V4.0 certification, the fact is that 3.0 has been archived for more than a year now. NIAP PP PSD V3.0 no longer reflects the government requirements for secure KVM switches in each security aspect, and there will be no new updates for 3.0-certified switches already in operation. Consequently, organizations considering their existing 3.0 KVM switches or looking at investment in new KVM switches need to determine if they can bear the risk sensitive data moving across a KVM system that doesn't meet the latest security norms.

Cybersecurity threats evolve quickly, requiring constant evaluation and improvement of security measures. NIAP PP PSD V3.0 is a 6-year-old protocol, and it cannot protect against the many new threats that have emerged since its publication. This is why cybersecurity specialists within government and military institutions have put forward new security features for NIAP PP PSD V4.0 certification and have made the new profile a standard requirement for procurement. NIAP PP PSD V4.0-certified secure switches are expected to complete evaluation and become available on the market as soon as Q3 2021.

The NIAP process for moving from one protection profile to the next includes a 6-month transition window during which a vendor can continue working toward certification with the earlier version. During this time, both PPs are available, and any vendor can continue on with 3.0, and it is still acceptable to deploy certified switches. After that window closes, however, the older version — PP 3.0 in this case — is archived, and the new version becomes the only valid PP. From that point forward, RFPs and other searches by government agencies (and likely many others) will call for NIAP PP PSD V4.0-certified devices.

Despite fact that the protection profile itself is no longer valid, a NIAP PP PSD V3.0 certification is good for the lifetime of the product. The many certified products in the field do not lose this status once 4.0 becomes the only current certification. They remain secure according to the requirements set out in PP 3.0. The risk that end users run in selecting these systems is that they haven't been evaluated against the government's latest security posture.

For some organizations, this level of risk is acceptable, and they will comfortably continue using deployed products for many years to come. But for organizations more sensitive to new and emerging cyber threats, the shift to NIAP PP PSD V4.0 is a smart choice — and is likely a mandatory part of any new equipment purchase.

By making it easier for individual operators to access the information they need to do their jobs efficiently, KVM technology plays a vital role in modern control rooms and other mission-critical areas of operations. KVM switches not only save space and improve workplace ergonomics but also support agility responsiveness in critical situations. NIAP PP PSD V4.0-certified secure KVM switches offer all of these essential benefits, as well as protection in accordance with current government requirements for cybersecurity.

Introducing first Secure KVM Switches in August 2008, Black Box has a 13 years tradition of providing high-performing secure KVM switches, and the company currently has a large range of switches undergoing NIAP PP PSD V4.0 evaluation. Whether for a new control room build, a facility update, or a KVM system refresh, Black Box has the technology and expertise to provide a flexible, reliable, and secure KVM system. Existing customers are still able to purchase NIAP 3.0 products, but for any new installations, NIAP 4.0 secure KVM switches will likely be the optimal and required choice.

Command and Control Room Solution

Large KVM matrix systems in a secure environment with multi-tiered access across enclaves with varying levels of security can be troublesome. Many potential problems arise when switching between these private, secure, or even top secret networks and open networks. Combining a KVM matrix and extension system like Black Box Emerald with a NIAP4 secure Defender can isolate single critical networks with all the benefits described in this whitepaper. This creates a solution that is specifically designed to meet secure end to end signal management at multiple classifications levels making it ideal for defence, government, military, intelligence, or any application in which security is a top priority. With this solution, hot, noisy and distracting workstations can be back-racked saving operator workspace therefore increasing productivity by reducing clutter.

Other options are mid-to-large scale fibre-optic KVM and video distribution systems certified to support multiple classifications through a single infrastructure. These high-end matrices have accreditation for Common Criteria EAL4, NATO (NIAPC) Green Status, JITC UCR and TEMPEST approval, while reducing interceptions with other networks or signal detection utlizing fiber cabling.

BLACK BOX
PC SELECTED
SECURE KVM SWITCH
DUAL-HEAD 4 PORT DP W/ AUDIO
SS4P-DH-DP-U

BLACK BOX