ATEN
Simply Better Connections

Strategic Cyber Defense Starts at the Desktop

Secure KVM Switches with NIAP PSD PP v4.0 Compliance Provide Hardware-Based Protection for a Multi-Network World

OVERVIEW

- **Cyber threats are accelerating in scale and complexity as hybrid work expands interconnected infrastructures.**

- **Hardware-based, NIAP-certified Secure KVM Switches are now essential for preventing data leakage between classified and non-classified networks.**

- **ATEN's PSD PP v4.0 Secure KVM portfolio provides multi-layered protection, up to 5K video performance, and strict peripheral control for government, defense, healthcare, finance, and critical infrastructure.**

- **With certified isolation and advanced physical safeguards, ATEN Secure KVM Switches deliver uncompromising security where it matters most: the desktop.**

Organizations today operate across increasingly interconnected networks, cloud environments, and remote endpoints—creating new vulnerabilities that cybercriminals actively exploit. The financial and operational impact of cyberattacks has reached historic levels, prompting governments and regulated industries to strengthen defenses across every layer of their infrastructure.

One area emerging as a priority is the desktop environment, where users often access multiple networks with different security classifications. Traditional software controls cannot fully prevent data crossover, peripheral-based threats, or unauthorized information flow between these networks. As a result, NIAP PSD PP v4.0–certified Secure KVM Switches have become a critical requirement for agencies and enterprises seeking guaranteed network separation and tamper-proof protection. ATEN's Secure KVM portfolio delivers this assurance through hardware-enforced isolation, multi-layer security mechanisms, strict peripheral filtering, and industry-leading 5K performance—making them the strategic choice for mission-critical desktop operations.

CONTENTS

1. Cyber Threats Evolve as Interconnectivity Reigns

Cybersecurity has reached a critical inflection point. As hybrid and remote work expand the number of connected devices, networks, and access points, organizations face a growing attack surface—one that cybercriminals are exploiting with unprecedented speed and sophistication. Threat actors now routinely target not only corporate data, but also critical infrastructure, financial systems, power grids, and global supply chains, turning isolated incidents into risks with national and economic impact.

The financial consequences are staggering. Cybercrime damages have soared past US$10.5 trillion annually, with forecasts warning of US$15.6 trillion by 2029[1]—exceeding the total losses from major natural disasters and surpassing the profits of global illicit markets. Government agencies and regulated industries are under increasing pressure to fortify the endpoints where sensitive data and human behavior intersect.

This pressure is accelerating the adoption of hardware-based security. The Secure KVM market alone is projected to grow from US$1.2 billion in 2024 to US$2.9 billion in 2033[2], driven by mounting requirements for NIAP-certified isolation, multi-network separation, and controlled peripheral access.

As organizations expand their security ecosystems—firewalls, SIEMs, identity and access platforms—many still overlook the highest-risk zone: the desktop, where users access classified and unclassified systems side by side. This is where a single data crossover, unauthorized peripheral, or malicious device can compromise national security or mission-critical operations.

NIAP-certified Secure KVM Switches have become a strategic safeguard for this environment. By enforcing strict hardware-level separation between networks, they eliminate entire classes of attack vectors that software-based tools cannot mitigate alone.

1. https://www.vikingcloud.com/blog/cybersecurity-statistics
2. https://www.verifiedmarketreports.com/product/secure-kvm-switches-market/

2. How Secure KVM Switches Can Help

Government agencies, critical infrastructure operators, and regulated enterprises routinely work across multiple networks with different security classifications. Yet many still rely on legacy systems, unmanaged peripherals, or policies that leave gaps at the desktop—the point where users interact with both sensitive and non-sensitive data.

Secure KVM Switches eliminate these vulnerabilities by enforcing **hardwired, NIAP-certified separation** between computers and user peripherals. Instead of relying on software controls, Secure KVMs provide trusted physical isolation that prevents data crossover, blocks unauthorized devices, and ensures that users cannot inadvertently transfer information between networks.

Whether in defense operations, healthcare research, financial trading floors, or corporate security centers, Secure KVM Switches deliver:

- **Controlled access** to multiple networks through a single workstation
- **Enforced one-way data flow**, preventing leakage between classified and unclassified systems
- **Protection against device-based attacks** through strict peripheral filtering
- **Operational efficiency** without reducing security posture

In environments where even a single user mistake or malicious device could create far-reaching consequences, Secure KVMs act as the **final safeguard**—ensuring that sensitive data remains protected at the hardware level.

> "Cybersecurity attacks are increasing each year. With this in mind, the government requires reassurance that if a peripheral sharing device or KVM is compromised, no usable data can be stolen from the device. NIAP-certified products are required to ensure that data leakage will not occur when switching between ports or classified to unclassified computers. Our PSD PP v4.0 Secure KVM Switch series limits the connection of devices at the desktop level, ensuring secure authentication and access that meet U.S. government and military mandates."
>
> *Aaron Johnson, KVM Product Manager*,
> **ATEN Technology, Inc., USA**

3. NIAP and PSD PP v4.0

The **National Information Assurance Partnership (NIAP)** establishes global standards for IT product security through the Common Criteria Evaluation and Validation Scheme (CCEVS). For Secure KVM Switches, NIAP's **Protection Profile for Peripheral Sharing Devices (PSD PP)** defines the requirements for preventing data leakage, protecting video interfaces, and maintaining strict control over peripheral behavior.

Why PSD PP v4.0 Matters

Introduced to meet updated security requirements for government, defense, and other high-security environments, **PSD PP v4.0** adds clearer assumptions, broader coverage of peripherals and interfaces, and more explicit evaluation criteria than those found in the earlier PSS PP v3.0. Key improvements include:

- Stricter device filtering for USB, keyboards, and mice
- Stronger audio isolation to prevent acoustic data leakage
- Updated testing coverage for advanced video formats and resolutions
- More robust tamper detection and hardware integrity checks
- Reinforced protections against malicious or emulated peripherals

These updates reflect the latest guidance for protecting classified environments and ensuring that no unauthorized data flow occurs across networks—particularly as users operate within increasingly connected workspaces.

NIAP certification provides clarity and trust: organizations can confidently deploy Secure KVM solutions knowing they meet validated, internationally recognized security standards.

NIAP for Trusted Secure KVM Certification

The National Information Assurance Partnership (NIAP) is a U.S. government initiative led by the National Security Agency (NSA), in cooperation with the National Institute of Standards and Technology (NIST). NIAP operates the Common Criteria Evaluation and Validation Scheme (CCEVS), which evaluates the security of commercial off-the-shelf IT products against internationally recognized Common Criteria standards. The program helps government agencies and security-sensitive organizations identify products that meet their required assurance levels.

Fig 1: The industry's first 5K Secure KVM Switches are available from ATEN. Model shown is the CS1184DPH4C 4-Port USB 5K DP/HDMI Universal Secure KVM Switch with CAC.

Why Hardware-Based Security Matters

Software alone cannot fully prevent data crossover, malicious peripherals, or user-driven mistakes in multi-network environments. **Hardware-based Secure KVM protection provides guarantees that software tools cannot:**

- **Immutable Security Controls**
  Hardware circuits enforce one-way data flow and isolation—no patches or updates can override them.
- **Protection against Device Spoofing**
  Malicious USB devices or emulated peripherals are blocked at the physical layer.
- **Guaranteed Network Separation**
  Dedicated internal data paths ensure no information can bridge classified and unclassified systems.
- **Tamper Resistance**
  Intrusion detection, ruggedized casing, and non-reprogrammable firmware prevent manipulation or compromise.
- **Zero Data Residue**
  Automatic keyboard/mouse data purging removes residual signals each time users switch networks.

Bottom line:
Where software can be bypassed, hardware locks down the desktop—providing the highest level of assurance in mission-critical environments.

4. The ATEN Secure KVM Solution

ATEN Secure KVM Switches deliver **high-assurance protection** for multi-network desktop environments by combining NIAP PSD PP v4.0 certification with advanced hardware security, strict peripheral control, and industry-first video performance.

As the first vendor to bring **5K Secure KVM Switches** to market, ATEN ensures that modern workstations in command centers, healthcare facilities, and financial institutions can maintain both **security and visual fidelity**—without compromise.

Built for High-Security Industries

ATEN Secure KVM solutions are trusted across:

- Government & Defense
- Healthcare & Medical Research
- Banking & Finance
- Critical Infrastructure
- Manufacturing & Industrial Control
- Corporate SOC and Risk Management Teams

Designed for Mission-Critical Operations

Each Secure KVM incorporates:

- Hardware-enforced network separation
- Multi-layer security, including tamper detection and non-reprogrammable firmware
- Configurable device filtering for CAC readers, keyboards, and mice
- Dual-monitor and 5K video options for high-resolution environments

ATEN Secure KVM Switches provide a **sealed, trusted path** between user controls and connected computers—ensuring data integrity, operational reliability, and compliance with international security standards.

5. Key Protections from ATEN for Instantly Secure Deployment

The ATEN Secure KVM Switch Series meets all key security requirements. They are designed to keep sensitive assets isolated while providing advanced security and a user friendly design for instantly secure deployment.

Multi-Layer Security

- Chassis intrusion detection
- Tamper-evident seals
- Non-reprogrammable firmware
- Restricted peripheral connectivity
- Secure port switching (pushbutton / RPS)
- Configurable Port LED color and Port Name Labels (Universal Series)
- Clear LED security status indicators
- Rugged metal enclosure
- Strict audio filtration

Data Channel Isolation

- Hardware-enforced separation
- Unidirectional data flow
- KB/MS data purging on KVM port change

Security Management

- USB CAC filtering
- Keyboard/mouse device filtering
- Audit logs
- Per-port CAC enablement

Superior Video Quality & Flexible Connectivity

- Up to 5K resolution (Universal Series)
- DP / HDMI combo connectors (Universal Series)
- Dual-monitor support
- ATEN Video DynaSync™ – Exclusive ATEN technology eliminates boot-up display problems and optimizes resolutions when switching among different sources

Fig 2: Thanks to its compact size, the ATEN PP4.0 Secure KVM Remote Port Selector (RPS) can be placed in line of sight on the desktop, enabling instant switching across multiple PCs and optimizing productivity while eliminating cable clutter.

7. Case Study: ATEN Secure KVM Solutions in Action

Multi-Layered Desktop Cybersecurity for a Government Agency

A major state-owned facility hosting multiple government branches sought to modernize its desktop security strategy. Employees routinely accessed networks with different classification levels—ranging from internal administrative systems to sensitive national infrastructure monitoring platforms. The organization needed a solution that would ensure complete isolation between networks while supporting both single- and dual-monitor configurations.

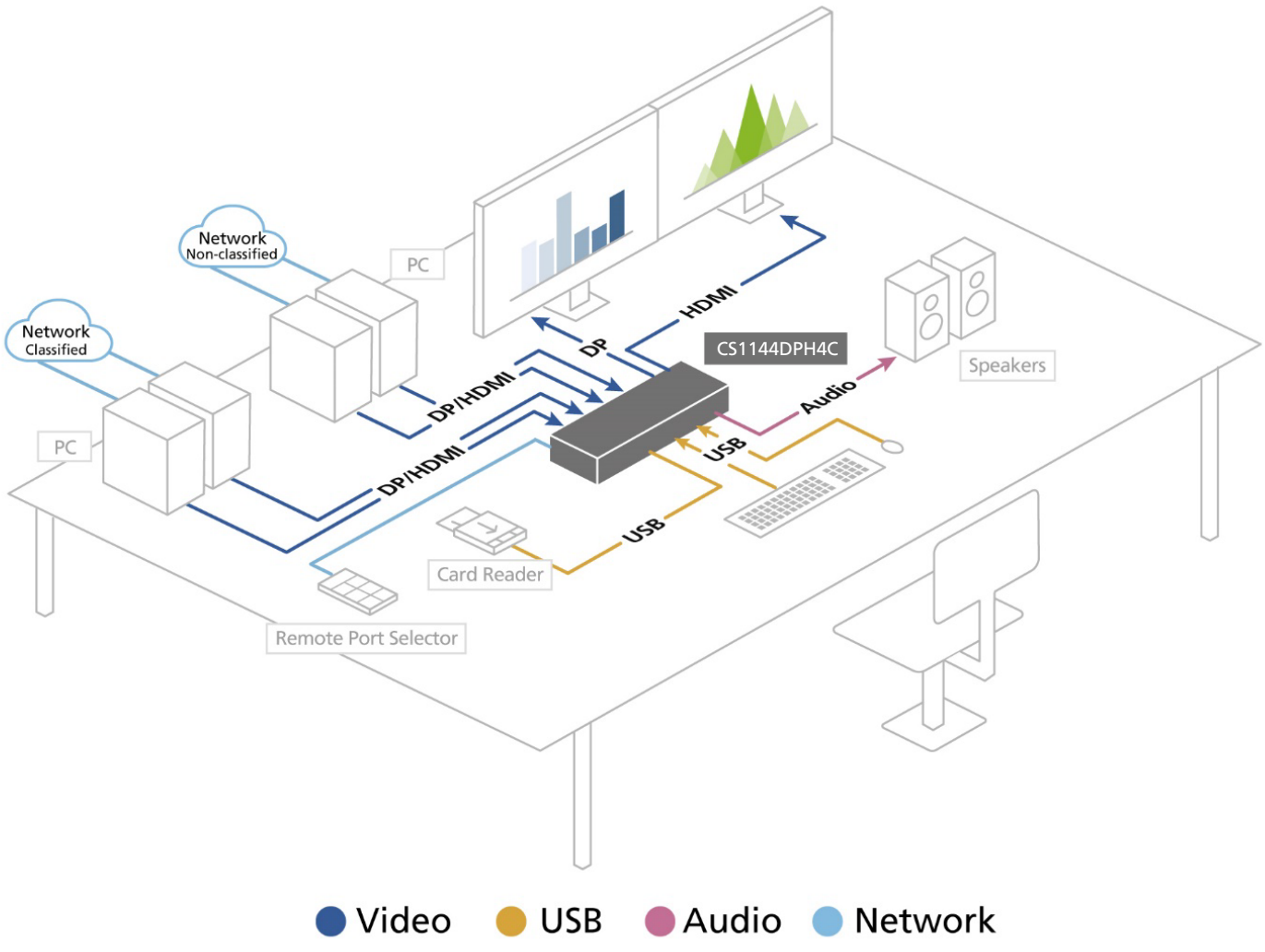
Challenges

- **Eliminate data crossover** between secure and unsecure networks
- **Guarantee strict channel isolation** to prevent accidental or intentional information transfer
- **Support both hardware and software-based security controls** at the desktop
- **Achieve compliance with NIAP PSD PP v4.0** to meet national cybersecurity mandates
- **Ensure system reliability** across multiple workstation types and user roles

The ATEN Solution

ATEN deployed PSD PP v4.0 Secure KVM Switches across the agency's offices, providing airtight, hardware-based separation between systems of varying security classifications. Through **tamper-proof construction, chassis intrusion detection, strict audio filtration, and configurable peripheral filtering**, ATEN's solution enabled the agency to maintain multi-level security with complete confidence.

By consolidating multiple networks into a single user console—while maintaining fully isolated data channels—the organization minimized its threat surface without compromising productivity. ATEN's Secure KVM Switches now serve as the agency's **last line of defense** at the desktop, protecting sensitive information and preventing data leakage across internal and external networks.



8. Making the Right Secure KVM Choice with ATEN

For government & military agencies, healthcare providers, banking & finance institutions, and more, looking for true network separation between classified and non-classified, and compliance with the latest international protection protocols, ATEN Secure KVM Switches provide an ideal solution. With protection on both the physical and user operation levels to combat data leakage across internal ports as well as to external networks, which can mitigate the vulnerabilities of a variety of cyber attacks, ATEN Secure KVM Switches are the strategic choice for security-conscious desktop applications across all industries. They are available in two series, as shown below:

ATEN PSD PP v4.0 Universal Secure KVM Switches

Featuring DP/HDMI combo connectors, secure port switching, strict audio filtration, configurable device filtration, and up to 5K video quality.

Up to 5K	CAC	2-Port		4-Port	
		Single Head	Dual Head	Single Head	Dual Head
Combo (DisplayPort / HDMI)	✓	CS1182DPH4C	CS1142DPH4C	CS1184DPH4C	CS1144DPH4C
	×	CS1182DPH4	CS1142DPH4	CS1184DPH4	CS1144DPH4

ATEN PSD PP v4.0 Secure KVM Switches

Featuring secure port switching, strict audio filtration, configurable device filtration, and up to 4K video quality.

Up to 4K	CAC	2-Port		4-Port		8-Port	
		Single Head	Dual Head	Single Head	Dual Head	Single Head	Dual Head
DisplayPort	✓	CS1182DP4C	CS1142DP4C	CS1184DP4C	CS1144DP4C	CS1188DP4C	CS1148DP4C
	×	CS1182DP4	CS1142DP4	CS1184DP4	CS1144DP4	CS1188DP4	CS1148DP4
HDMI	✓	CS1182H4C	CS1142H4C	CS1184H4C	CS1144H4C	N/A	N/A
	×	CS1182H4	CS1142H4	CS1184H4	CS1144H4	N/A	N/A
DVI	✓	CS1182D4C	CS1142D4C	CS1184D4C	CS1144D4C	CS1188D4C	CS1148D4C
	×	CS1182D4	CS1142D4	CS1184D4	CS1144D4	CS1188D4	CS1148D4

For more information about ATEN's PSD PP v4.0 Secure KVM Switches, please visit
https://www.aten.com/global/en/product-landing-page/secure-kvm-series/