Cybersecurity Concerns?

Make the Strategic Choice for Secure Government and Military Desktops

Secure KVM Switches with NIAP PSS PP v3.0 Compliance are Equipped to Secure the Desktop while Providing an Unparalleled User Experience

January 2019

CONTENTS

1. Introduction

Cybersecurity is on everyone's mind these days and with good reason: it's a growing threat that many organizations are unprepared to face, especially governments. However it's in their best interest to establish robust cybersecurity measures, considering cyber-attacks cost the global economy about US$600 billion in 2017, according to McAfee and the Center for Strategic and International Studies (CSIS)[1]. Hackers, from independent ones to terrorists and those working for foreign governments, are responsible for ransomware, distributed denial of service, and stealing of classified information. What's worse, the *Cisco 2018 Annual Cyberspace Security Report*[2] found cyberattacks are expected to increase in 2019 and are growing more sophisticated by the day. Welcome to the future of warfare, fought safely from behind a keyboard.

Many government agencies are still lacking when it comes to cybersecurity. For example: the US government only just established its first cybersecurity agency in late 2018. The UK's government revealed around the same time that it was ill-equipped to deal with cyber-attacks on its national infrastructure, including power grids. That means hackers could potentially shut down power to large portions of the UK. The nation is now considering creating its first cybersecurity minister.

2. Is Your Cyber Backdoor Wide Open?

Risk management firm SecurityScorecard noted in 2017 that many US government agencies struggled with basic cybersecurity measures, from reusing older passwords on management accounts, to devices exposed to the public Internet. Internet of Things (IoT) devices were especially poorly managed, and thus exposed, often undetected by agencies. Simply put, many are leaving the door wide open for hackers, terrorists, and other cyber criminals.

The good news? All of these problems are relatively simple to solve. The key is to be proactive instead of reactive. Replacing legacy technology that has long since been figured out by hackers is one of the first things government agencies can do.

3. Secure KVM Switches to the Rescue

With cyber threats growing every year, a robust solution needs to meet them head-on. Enter Secure KVM solutions. Security-reinforced KVM switches provide the means to consolidate multiple workstations of various security classification levels with a single keyboard, monitor, and mouse also known as a KVM console. With hardware and software-based security features built into the units, military, intelligence, and federal agency installations can rest assured that their data is being protected on both physical and digital levels.

NIAP for Trusted Secure KVM Certification

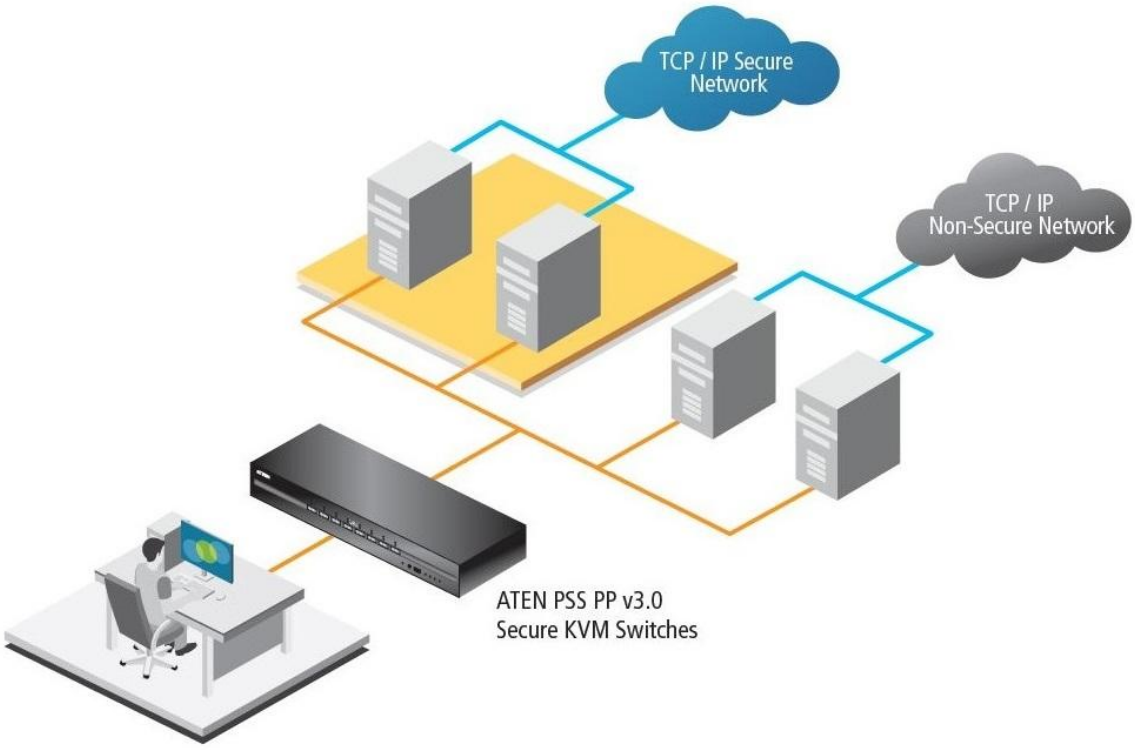
The National Institute of Standards and Technology (NIST) and the National Security Agency (NAS) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product performance to international standards. The program, known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS), was implemented to help consumers and government agencies select commercial off-the-shelf IT products that meet their security requirements.

4. The ATEN Secure KVM Solution

ATEN has expanded its enterprise KVM solutions with the launch of a new series of Secure KVM switches. With a complete product lineup (2/4/8-port USB DVI/HDMI/DisplayPort Single/Dual Display models are available) and superior video quality (resolutions up to 3840 x 2160@30Hz with crystal clear image quality are supported), all ATEN secure KVM switches are compliant with PSS PP v3.0 (Protection Profile for Peripheral Sharing Switch, Version 3.0) certified by the National Information Assurance Partnership (NIAP). This ensures high-level desktop security, protection and data safekeeping for organizations in industries such as government agencies (e.g. Department of Defense, Department of Justice, CIA, military, etc.), financial institutions and any other environment that uses multiple computers of different security levels shared within peripheral sharing switches or KVM's.

ATEN's PSS PP v3.0 Secure KVM Switches provide isolation between computer sources and peripherals while sharing a single keyboard, mouse, monitor, speakers, and Common Access Card (CAC) reader between connected computers of various security classifications. Compliance with PSS PP v3.0 ensures peripheral sharing capabilities provide maximum user data security when switching port focus, preventing unauthorized data flows or leakage between connected sources. Key protections include isolation and unidirectional data flow, restricted peripheral connectivity and filtering, user data protection, configurable device filtering and management, and tamper-proof design, keeping sensitive assets isolated and providing advanced security and a user-friendly design for instantly secure deployment.

Secure KVM desktop access to computers at multiple classification levels.



5. Key Protections from ATEN for Instantly Secure Deployment

The PSS PP v3.0 Secure KVM Series from ATEN meet all security requirements. They are designed to keep sensitive assets isolated while providing advanced security and a user friendly design for instantly secure deployment.

- **Secure Port Switching** — Port selection via pushbutton only to enhance security.
- **Data Channel Isolation** — Isolated channel per port to prevent data leakage between connected computers.
- **Restricted USB connectivity** — Non-authorized HIDs (Human Interface Devices) or non-predefined CAC devices will be rejected / ignored.
- **User Data Protection** — Keyboard/Mouse data buffer is automatically purged when switching KVM port focus.
- **Configurable Device Filtering** — USB CAC Port can be configured to allow/reject whitelisted/blacklisted devices via Admin logon function or Windows-based application.
- **Administrator Configuration and Event Log Functions** — User friendly interface for authorized administrator to audit critical KVM operation logs and perform KVM switch configuration.
- **Always-on Tamper-proof Design** — The KVM switch becomes inoperable when physical tampering is detected.

ATEN's PSS PP v3.0 Secure KVM Switches support different customer demands, with options including 2-port, 4-port and 8-port models, and video interfaces including DisplayPort, HDMI, and DVI. The ATEN series of Secure KVM Switches also provides customers with the flexibility to connect single or dual displays, providing up to 4K UHD (3840 × 2160 @30Hz) video quality.

> *"Cybersecurity attacks are increasing each year. With this in mind, the government requires reassurance that if a peripheral sharing switch or KVM is compromised, no usable data can be stolen from the device. PSS PP v3.0 certified products are required to ensure that data leakage will not occur when switching between ports or classified to unclassified computers. Our new PSS PP v3.0 Secure KVM Switch series limits the connection of devices at the desktop level, ensuring secure remote authentication and access that meet U.S. government and military mandates."*
>
> **Aaron Johnson, KVM Product Manager,**
> **ATEN Technology, Inc., USA**

6. Making the Right Secure KVM Choice with ATEN

For government and military agencies looking for true network separation between classified and non-classified, and compliance with the latest international protection protocols, the ATEN PSS PP v3.0 Secure KVM Series provides 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 in all industries.

For more information about ATEN's PSS PP v3.0 Secure KVM Series, please visit https://www.aten.com/global/en/products/kvm/secure-kvm-switches/

.

ATEN PSS PP v3.0 Secure KVM Series Models

PC Video Connection	Console Video Connection	No. of Displays	2-Port	4-Port	8-Port
DisplayPort	HDMI	Single	CS1182DP	CS1184DP	CS1188DP
		Dual	CS1142DP	CS1144DP	CS1148DP
HDMI	HDMI	Single	CS1182H	CS1184H	CS1188H
		Dual	CS1142H	CS1144H	CS1148H
DVI	DVI	Single	CS1182D	CS1184D	CS1188D
		Dual	CS1142D	CS1144D	CS1148D

Reference Notes

1. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

2. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf