ATEN
Simply Better Connections

사이버 보안 위협에 대처하는 최적의 전략

NIAP PSD PP v4.0 / PSS PP v3.0으로
보안 데스크탑 워크스테이션을 구축하는 보안 KVM 스위치

목차

1. 업무 환경 변화에 따른 사이버 위협의 증가

오늘 날 많은 사람들이 여러 가지 이유로 사이버 보안에 대해 우려합니다.
하이브리드 및 원격 작업이 늘어나면서 상호 연결되고 여러 사람, 기업, 시스템과 협업하는 상황이 생겨나면서 사이버 공격 기회가 증가하고 있기 때문입니다. 포브스(Forbes)[1]에 따르면 2021년 솔라 윈즈(Solar Winds)나 콜로니얼 파이프라인(Colonial Pipeline)과 같이 세간의 이목을 끄는 보안 침해 사건이 많이 발생했지만, 가장 우려되는 것은 중요 인프라, 전력망, 공급망의 보안 취약점이 과거보다 훨씬 더 높은 비율로 사이버 공격의 표적이 되고 있다는 점입니다.

이러한 위협은 점차 진화하고 있으나 많은 기업들, 특히 일부 정부 기관은 사이버 위협에 대한 대비가 미흡합니다. 이에 따라 강력한 사이버 보안 대책을 수립하는 것이 필요하며, 사이버 시큐리티 벤처(Cybersecurity Ventures)[2]의 연구에 따르면 사이버 범죄로 인해 2025년까지 전 세계적으로 연간 10조 5000억 달러의 피해가 예상되며 이는 역사적으로 가장 큰 경제 규모라고 합니다. 이 금액은 1년 동안 자연재해로 인한 피해보다 훨씬 큰 규모이며 모든 주요 불법 약물의 세계 거래량의 수익보다 더 많은 것이라고 합니다.

독립적인 해커에서 테러리스트, 외국 정부를 위해 일하는 해커에 이르기까지 랜섬웨어, 분산 서비스 거부, 기밀 정보 도용 등 다양한 공격을 합니다. 하지만 대부분의 사이버 보안 제공 업체는 특정 업종을 전문으로 하여 고객이 서로 다른 기업의 패치워크를 사용하여 데이터를 보호하도록 합니다. 이는 지속적으로 진화하는 사이버 공격에 효과적인 대비가 아니며 더욱 확실하고 강화된 보안이 필요합니다.

1. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity
2. https://cybersecurityventures.com/cybersecurity

2. 보안 KVM 스위치 활용 방법

오래 전부터 정부 기관은 사이버 위협에 노출되어 있으나 관리 계정의 이전 비밀 번호 재사용이나 공공 인터넷에 노출되는 장치에 이르기까지 기본적인 사이버 보안 관리에 대한 어려움을 여전히 겪고 있습니다. 사물 인터넷(IoT) 장치는 특히 제대로 관리되지 않아 기관에서 감지하지 못하는 경우가 많습니다. 간단히 말해서, 구식 프로토콜과 기술에 익숙하지 않은 인력이 해커, 테러리스트, 사이버 범죄자들에게 문을 활짝 열어 놓고 있는 것과 같다고 할 수 있습니다. 하지만 이 모든 문제들을 해결할 수 있는 비교적 간단한 방법이 있습니다. 핵심은 사후 대응이 아닌 사전 예방입니다. 해커에게 이미 잘 알려진 기존 시스템을 교체하는 것은 정부 기관이 할 수 있는 가장 첫 번째 단계의 보안입니다. 그러나 다음 단계의 사이버 보안은 어떻게 해야 할까요?

물리적 & 디지털 보호

보안 KVM은 사이버 보안에 대응할 수 있는 확실한 솔루션입니다. 보안 강화 KVM 스위치는 다양한 보안 기밀 단계의 멀티플 워크스테이션을 KVM 콘솔(키보드, 모니터, 마우스) 하나로 통합하는 솔루션을 제공합니다.
또한 군, 정보 기관, 정부 기관 설비에 하드웨어와 소프트웨어 기반의 보안 기능을 구축해 물리적 그리고 디지털 단계로 데이터를 안전하게 보호합니다. 정부 기관 뿐만 아니라 아닌 다른 기관에서도 솔루션의 특징을 적용할 수 있습니다.

의료 관계자는 환자 개인 정보와 같은 예민한 정보와 보험과 같이 상대적으로 덜 예민한 정보를 동시에 취급해야 합니다. 금융 분야에서는 은행이 여러 시장으로 통합됨에 따라 망분리된 컴퓨터와 망분리되지 않은 컴퓨터를 구분하는 네트워크 분류에 대한 필요성이 증가하고 있습니다. 보안 KVM 스위치는 사용자 콘솔 스테이션에 물리적 보안 수준을 제공하여 네트워크를 격리하고 허가되지 않은 사용자의 손에 정보가 들어가는 것을 방지합니다.
이것은 내부 위협에 대한 데스크탑의 마지막 방어입니다.

"사이버 보안 공격은 해마다 증가하고 있습니다. 이 점을 염두에 두고 정부는 공유 스위치 또는 KVM에 사이버 공격이 있을 경우 데이터가 유출되지 않도록 요청했습니다. PSS 인증 제품은 포트 간 전환 또는 미분류 컴퓨터로 분류 시 데이터 누출이 발생하지 않아야 합니다.
우리의 새로운 PSD PP v4.0 보안 KVM 스위치 시리즈는 데스크탑 수준에서 장치 연결을 제한하여 미국 정부 및 군사 규정을 충족하는 안전한 원격 인증 및 접근을 보장합니다."

애론 존슨, KVM 제품 매니저
ATEN Technology, Inc., USA

3. NIAP의 PSD PP v4.0 도입

국가 정보 보증 파트너쉽(NIAP)은 미국 국립 표준 기술원 (NIST)과 공동으로 공통 평가 시험 및 인증을 시행하는 규제 기구입니다. NIAP는 국제 상호 인정 협정의 31개 회원국 중 미국 대표의 역할을 하고 있습니다. 이 협정의 목적은 IT 제품 평가이며, 높은 수준과 일관된 기준으로 실행되는 보호 프로파일은 인증된 제품에 높은 신뢰성을 부여합니다. 2015년 이후 PSS PP v3.0 (주변장치 공유 스위치에 대한 보호 프로파일)은 전세계 시장에서 보안 KVM 스위치가 갖추어야 할 필수 인증이 되었습니다.

시대가 변화하면서 사이버 보안 위협은 더욱 커졌습니다. 2020년, NIAP는 미국 정부가 신중하게 고려한 보안 요구사항을 반영해한 업데이트 버전의 SD PP v4.0 (주변장치 공유 스위치에 대한 보호 프로파일)을 도입했습니다. 사이버 테러와 범죄에 대비한 앞선 보안 기술을 위해 지속적인 재평가와 업데이트가 이루어 졌으며 최근 몇 년간 드러난 위협 요인의 여러 가지 유형을 겨냥한 최신 보호 프로파일을 선보였습니다.
현재의 보안 약점 중 상당 부분은 COVID-19 위기에 대응하기 위해 전세계 업무 환경이 효율성과 협업 향상으로 전환하면서 생겨난 것으로 해커들은 산업마다 다른 보안의 약점과 차이를 교묘하게 이용했습니다.
이런 상황 역시 많은 기관이 여전히 사이버 보안에 준비가 되지 않았음을 보여줍니다.

신뢰성 있는 보안 KVM 인증 NIAP

미국 국립 표준 기술원 (NIST)과 미국 국가 안전국 (NSA)는 국가 정보 보증 파트너쉽(NIAP) 산하의 프로그램을 구축해 국제 표준에 맞는 IT 제품 성능을 평가합니다. NIST와 NSA는 고객과 정부 기관이 보안 요구 조건에 부합하는 상용 제품을 고르는데 기준이 될 수 있도록 NIAP 보안적합성심사제도 (CCEVS)라고 알려진 프로그램을 실행합니다.

4. ATEN 보안 KVM 솔루션

ATEN은 보안 KVM 스위치의 새로운 시리즈를 출시해 엔터프라이즈 KVM 솔루션을 확장했습니다.
ATEN 보안 KVM 스위치는 공통 평가와 NIAP 보호 프로파일 (PSD PP v4.0, PSS PP v3.0)을 준수합니다.
특히 민감한 자산을 분리하여 엄격하게 데스크탑 보안을 실행하도록 고안되었으며, 최신 사용자 데이터 보호와 유연한 보안 관리 기능을 제공합니다. 이 솔루션은 민감하고 기밀로 보호해야 하는 정보를 처리 하거나 정부, 군, 의료, 은행& 금융 기관 등과 같이 별도의 네트워크 상에서 다양한 보안 권한을 실행해야 하는 모든 산업의 환경에 알맞습니다.

ATEN PSD PP v4.0 보안 KVM 스위치는 콘솔 장치와 연결된 컴퓨터 사이의 데이터 흐름을 제어하고 분리합니다.

일반 기준 준수

ATEN 보안 KVM 스위치는 PSDPP v4.0(주변장치 공유 장치에 대한 보호 프로파일) 및 PSSPP v3.0(주변장치 공유 스위치에 대한 보호 프로파일)을 준수합니다. 다양한 보안 권한으로 연결된 컴퓨터를 단일 키보드, 마우스, 모니터, 스피커, 공통 접속 카드 리더로 공유하면서 컴퓨터 소스와 주변 장치를 격리하여 정보 보안을 최대로 보장합니다.

강력한 보안

ATEN 보안 KVM 스위치는 격리 및 단방향 데이터 흐름, 제한된 주변 장치 연결, 필터링 사용자 데이터 보호 구성 가능한 장치 필터링을 포함한 주요 보호 기능을 제공합니다.
또한 민감한 자산을 유지하고 즉각적인 보안 배포를 위한 고급 보안이 사용자 친화적인 디자인으로 적용되었습니다.

5. 즉각적인 보안 환경 구축을 위한 주요 기능

ATEN의 보안 KVM 스위치 시리즈는 주요 보안 요구사항을 충족합니다. 보안 설비에 민감한 정보를 즉각적으로 분리하며 최신 보안 기능과 사용자 친화적인 디자인을 제공합니다.

멀티 레이어 보안

- **상시 침입 감시** – 물리적 간섭이 감지되면 ATEN 보안 KVM 스위치의 동작이 불가합니다.
- **침입 증거 리포트** – ATEN 보안 KVM 스위치의 내부 구성 요소에 접속하기 위한 모든 시도의 시각적 정보를 제공합니다.
- **펌웨어 재프로그래밍 방지** – ATEN 보안 KVM 스위치의 펌웨어 재프로그래밍을 방지합니다.
- **물리적 연결성 제한** – 미승인 HID (Human Interface Devices), 비디오 또는 인증 장치 연결이 거부됩니다.
- **안전한 포트 전환** – 보안 (PSD PP v4.0 모델 한정)을 강화하는 푸쉬 버튼 / 원격 포트 선택기 (RPS)를 제공합니다.
- **명확한 LED 표시** – 주변장치 필터링 및 KVM 보안 상태를 LED로 표시합니다.
- **견고한 금속 마감**
- **강력한 오디오 필터링** – 오디오 유출을 방지합니다. (PSD PP v4.0 모델 한정)

작은 크기로 ATEN PP4.0 보안 KVM 원격 포트 선택기(RPS)를 데스크탑의 가시 거리 내 배치할 수 있으며 복잡한 케이블 설치 없이 다수의 PC 사이를 즉각적으로 전환하고 생산성을 극대화할 수 있습니다.

데이터 채널 분리 및 단방향 데이터 흐름

- 실제 데이터 경로 분리 – 컴퓨터 사이의 데이터를 전송할 수 없습니다.
- ATEN 보안 KVM 스위치는 콘솔 장치와 연결된 컴퓨터 사이의 데이터 흐름을 제어하고 분리합니다.
- 콘솔 장치와 선택한 컴퓨터 사이의 단방향 데이터 흐름을 보장합니다.
- 아날로그 오디오를 지원합니다. (스피커 한정)

사용자 데이터 보호

전송 후 보안 KVM 스위치의 키보드/마우스 데이터를 자동으로 삭제하며 KVM 포트 포커스를 전환할 때 자동으로 삭제합니다.

보안 관리

- 특정 USB 인증 장치(PSD PP v4.0 CAC 모델 및 PPS PP v3.0 모델 한정)를 허용하거나 거부하는 CAC 포트 필터링의 관리상의 구성을 지원합니다.
- 특정 USB HID 장치 (PSD PP v4.0 모델 한정)를 거부하는 키보드/마우스 포트 필터링의 관리 구성을 지원합니다.
- 승인 받은 관리자에게 관리 기능을 제공해 KVM 로그 데이터 회계 감사를 할 수 있습니다.
- CAC 기능을 포트(PSD PP v4.0 CAC 모델 및 PPS PP v3.0 모델 한정) 별로 활성화/비활성화 할 수 있습니다.

우수한 화질

- **4K 이미지 품질**
  최대 3840 x 2160 @60Hz (PSD PP v4.0 모델) 및 3840 x 2160 @30Hz (PSS PP v3.0 모델)의 이미지 해상도를 지원합니다.
- **듀얼 디스플레이**
  2대의 모니터로 비디오 출력을 매끄럽게 표시할 수 있습니다.
- ATEN Video DynaSync™
  독점 ATEN 기술로 다양한 소스 사이를 전환할 때 디스플레이 부팅 문제를 없애고 해상도를 최대화 합니다.

6. PSS PP v3.0와 PSD PP v4.0의 차이점

최신 PSD PP v4.0 프로필의 주요 조항은 2015년 이후 재평가 및 개선의 결과로 미국 정부가 신중하게 고려한 보안 요구사항에 대한 필수 업데이트를 반영합니다.
예를 들어, 새로운 비디오 인터페이스가 허용되고 비디오 인터페이스의 특정 프로토콜이 테스트 절차에 포함되며 오디오 필터링에 대한 더 엄격한 평가를 진행했습니다.

PSD PP v4.0 모델은 미국 정부 기준 인증에 맞는 가장 최신 NIAP 요구사항을 충족하며, 인증된 PSD PP v3.0 모델 또한 여전히 장치 수명 동안 관련된 모든 요구사항을 충족합니다. 다양한 환경에 맞는 우수하고 완전한 보안을 제공하므로 우려할 부분은 없습니다.

ATEN의 보안 KVM 스위치에 대한 내용은 다음 표에서 구체적으로 제공합니다.
ATEN의 PSD PP v4.0 및 PSS PP v3.0 간 주요 차이점을 확인하십시오 :

	PSD PP v4.0	PSD PP v3.0
보안 포트 선택	푸쉬 버튼, 원격 포트 선택기 (RPS)	푸쉬 버튼
견고한 오디오 필터링	v	x
키보드/마우스 포트에서 구성 가능한 장치 필터링	v	x
비 CAC 모델 지원	v	x
미인증 USB HID 연결에 대한 LED 표시	v	x
4K UDH 화질	최대 3840 x 2160 @60Hz	최대 3840 x 2160 @30Hz

7. 케이스 스터디: ATEN 보안 KVM 솔루션

정부 기관용 데스크탑의 다중 사이버 보안

다수의 정부 기관이 입주한 대형 건물에서는 싱글 및 듀얼 모니터 설비가 혼합된 다양한 보안 수준의 워크스테이션 여러 대를 통합해, 외부 위협을 방어하고 견고한 사이버 보안을 구축할 수 있는 방법을 찾고 있었습니다.
일반 데스크탑 KVM 스위치와 유사하지만 전력망과 같은 국가 인프라에 대한 잠재적인 사이버 공격으로부터 보호하는데 도움이 되는 데스크탑 솔루션이 필요했습니다. 따라서 기밀 데이터와 비 기밀 데이터 채널 사이의 실제 네트워크 분리를 제공하고 최신 국제 보호 프로토콜을 준수하는 솔루션이 반드시 있어야 했습니다.

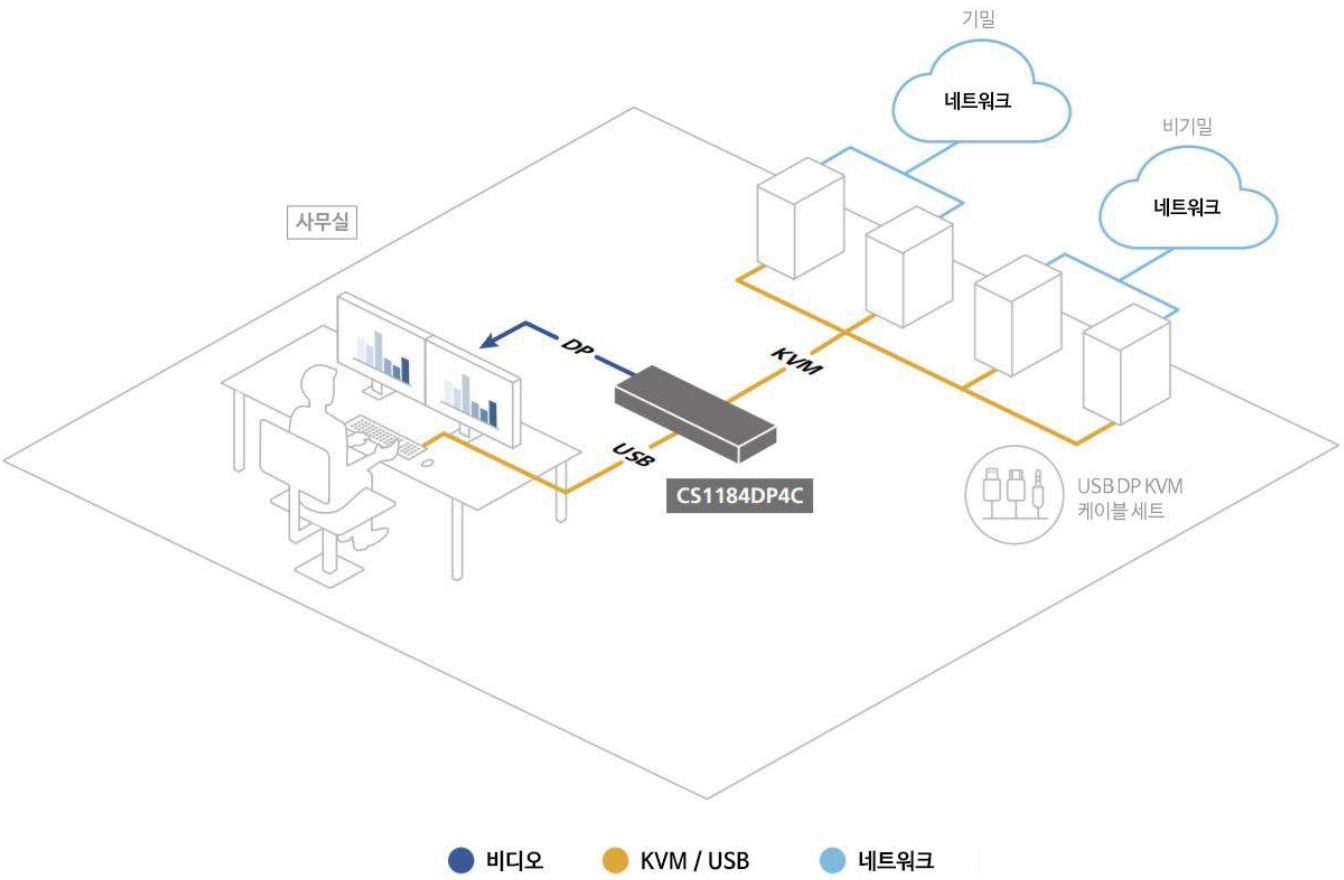
요구 사항 :

- 보안 또는 비 보안 네트워크에 접속하는 데스크탑 간 데이터 통합으로 보안 위협을 최소화합니다.
- 컴퓨터 간 데이터 전송이 불가능하도록 채널을 분리합니다.
- 하드웨어와 소프트웨어 기반 보안 기능을 제공합니다.
- PSD PP v4.0 (주변장치 공유 스위치에 대한 보호 프로파일) 보안 요구사항을 준수합니다.

ATEN 솔루션

ATEN 솔루션으로 정부 기관은 최신 사용자 데이터 보호와 유연한 보안 관리 기능을 제공하면서 별도로 네트워크에 민감한 자산을 분리해 데스크탑에서 강력한 멀티 레벨 보안을 실행할 수 있습니다.

견고한 오디오 필터링, 키보드/마우스 포트의 구성 가능한 장치 필터링, 섀시 침입 감지 및 소프트웨어 보안 레이어와 결합해 쉽게 변경할 수 없는 하드웨어로 다양한 사이버 공격의 취약점을 완화합니다. ATEN 보안 KVM 스위치는 물리적 및 디지털 단계의 다중 보호 기능으로 군 수준의 보안 기능을 제공해 인터넷 포트와 외부 네트워크 상의 데이터 유출을 방지합니다.



8. 올바른 보안 KVM 선택을 위한 ATEN의 제안

기밀 및 비기밀 사이의 실제 네트워크 분리와 최신 국제 보호 프로토콜을 준수하는 솔루션을 찾는 정부 & 군 관련 기관, 의료 업계, 은행&금융 기관 등에게 ATEN 보안 KVM 스위치는 이상적인 솔루션을 제공합니다.
물리적 및 사용자 동작 단계에 모두 보호 기능을 제공해 인터넷 포트 및 외부 네트워크 상의 데이터 유출에 대항하여 다양한 형태의 사이버 공격의 취약성을 완화시킵니다. ATEN 보안 KVM 스위치는 모든 산업 환경에서 보안 우려가 있는 데스크탑에 가장 전략적인 선택입니다.

ATEN PSD PP v4.0 보안 KVM 스위치

		2-포트		4-포트		8-포트	
	CAC	싱글 헤드	듀얼 헤드	싱글 헤드	듀얼 헤드	싱글 헤드	듀얼 헤드
DisplayPort	v	CS1182DP4C	CS1142DP4C	CS1184DP4C	CS1144DP4C	CS1188DP4C	CS1148DP4C
	x	CS1182DP4	CS1142DP4	CS1184DP4	CS1144DP4	CS1188DP4	CS1148DP4
HDMI	v	CS1182H4C	CS1142H4C	CS1184H4C	CS1144H4C	N/A	N/A
	x	CS1182H4	CS1142H4	CS1184H4	CS1144H4	N/A	N/A
DVI	v	CS1182D4C	CS1142D4C	CS1184D4C	CS1144D4C	CS1188D4C	CS1148D4C
	x	CS1182D4	CS1142D4	CS1184D4	CS1144D4	CS1188D4	CS1148D4

ATEN PSS PP v3.0 보안 KVM 스위치

		2-포트		4-포트		8-포트	
	CAC	싱글 헤드	듀얼 헤드	싱글 헤드	듀얼 헤드	싱글 헤드	듀얼 헤드
DisplayPort	v	CS1182DP	CS1142DP	CS1184DP	CS1144DP	CS1188DP	CS1148DP
HDMI	v	CS1182H	CS1142H	CS1184H	CS1144H	CS1188H	CS1148H
DVI	v	CS1182D	CS1142D	CS1184D	CS1144D	CS1188D	CS1148D

ATEN의 PSD PP v4.0 / PSS PP v3.0 보안 KVM 스위치에 대한 상세 내용은 ATEN Korea 영업 담당자에게 문의하십시오.