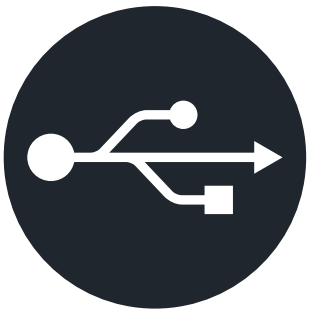
엔드포인트 보안의 성능 저하 없이

# USB 드라이브에 액세스하는 법

#KingstonIsWithYou #KingstonIronkey

# 소개

1996년 1월, 공식 USB 1.0의 출시 사양은 주변 장치 공급자와 사용자 모두에게 통일성과 편의성, 범용성의 새 시대를 예고했습니다. 27년 후에도, 각 개정판 간의 호환성을 유지하면서 USB는 서버부터 스마트폰에 이르기까지 컴퓨터 하드웨어 인터페이스의 주춧돌 역할을 유지하고 있습니다.



USB의 플러그앤플레이 편이성과 날로 빨리지는 속도를 기반으로 USB 휴대용 스토리지는 엄청나 수익을 거두는 상품으로 발전하게 되었습니다. 하지만 그런 편이성은 데이터 보안에 있어서는 양면성을 지닙니다. 오늘날 호스트 컴퓨터에서 엔드포인트 보호와 같은 적절한 도구와 적절한 데이터 보안 관행을 사용하지 않고 휴대용 USB 스토리지를 사용하는 부주의한 태도를 가진 사용자는 자신과 타인을 데이터 유출 가능성에 노출시켜 최종 사용자에게 막대한 비용을 초래하고 심지어 조직이나 정부 전체를 위험에 빠뜨릴 수 있습니다.

호스트 환경을 보호하는 것과 함께, 비밀번호 보호와 장치 하드웨어 암호화를 통해서도 USB 드라이브의 보안을 유지해야 합니다. 이것이 침입에 대비하는 가장 강력한 방어입니다. 당사는 USB 드라이브에 대한 보다 전반적인 면밀한 검토와 더불어 USB 드라이브를 보다 보안이 되는 방식으로 사용하기 위한 몇 가지 가장 우수한 관행을 살펴보겠습니다.

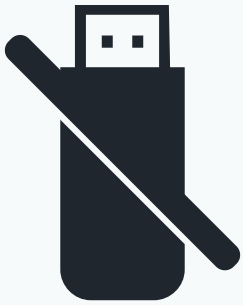
복합적인 접근법인 이상적인 반면, 이 접근법에서 가장 중요한 것은 강력한 암호화와 USB 드라이브 자체의 하드웨어 부품입니다. 이런 장점들은 금융에서 의료, 제조 및 국방에 이르는 분야에 영향을 미칩니다. 또한 네트워크에 액세스할 수 없거나 액세스가 취약하거나 현실적으로 불가능한 경우의 원격 작업에서도 중요한 역할을 합니다.

USB 암호화 하드웨어 드라이브는 광범위한 보안 기능과 함께 다양한 인증 등급을 제공합니다. 사용자 설정에 대한 속성과 기회를 살펴보면, 모든 민감한 환경에서 독립형 솔루션으로서 그것들이 가지는 적합성은 그들의 위치를 보호함으로써 드러납니다.

# 포트 사용 권한: USB 저장 장치와 엔드포인트 관리 데이터 손실 방지 소프트웨어와의 결합

수십 년간, 바이러스 백신과 멀웨어 차단 어플리케이션은 가장 기초적인 수준의 보안만을 제공해왔습니다. 다운로드와 보조 장치를 자동 스캔하거나 의심스러운 내용을 보고하고 작동하는 정도였습니다. 차세대 바이러스 백신(Next Generation Anti-Virus/NGAV) 소프트웨어의 보안은 한 단계 발전합니다. 계속해서 발전하는 바이러스 시그니처의 데이터베이스에 의존하지 않고, NGAV에는 미지의 위협을 감지하고 완화시킬 수 있는 행동 감지 특성과 머신 러닝이 더해졌습니다.

병기창에 한 가지 무기만 있는 것이 아닙니다. 사용자의 주변 장치 등으로부터 날아오는 총알로부터 막아내기를 원하는 사람들을 위해서 엔드포인트 관리 데이터 손실 방지(Endpoint Management Data Loss Prevention/DLP) 소프트웨어는 USB 포트와 기타 액세스 지점에 대한 모든 종류의 액세스를 막아낼 수단을 제공합니다.



보안에 대해 모든 포트 차단과 같은 태도는 바라건대 몇몇 상황에서는 분명히 위험을 제거할 수 있습니다. 하지만 그런 방식은 종종 밝혀진 증거에 따르면 매우 무딘 도구여서 바라지 않는 결과를 초래할 수도 있습니다.

그럼에도 몇몇 IT 운영자들은 사용자 기계에서 USB 포트를 개방해달라는 요청이 줄어들었으면 하고 생각합니다. 그렇게 되면 이런 엔드포인트들은 기업 방화벽에 직접적인 액세스를 허용하기 때문입니다. 그런 걱정이 이해가 되지 않는 것은 아닙니다. 하지만 USB 저장 장치에 대한 액세스를 허용할 때에 특정 선행 조건이 준수된다면 이런 권한을 부여하는 것이 보안상 큰 골칫거리가 되지는 않아야 합니다.

조건으로는 전체 사용자 엔드포인트의 중앙 모니터링 및 관리와 바이러스 백신/멀웨어 차단에 대한 위험 감지 스캔이 가능한 엔드포인트 관리 어플리케이션 제품군이 필요합니다.

이런 단순한 접근법은 다양한 모습으로 통합 솔루션을 제공합니다. 유명한 업체를 조금만 나열하자면 McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection and WinMagic SecureDoc 등이 있습니다.

# 화이트 리스트 개선


USB 저장 장치를 보호함에 있어서 사용되는 방법은 필요한 보호 수준에 따라 다릅니다. 간단하지만 효과적인 접근법으로는 USB 저장 장치 각각의 업체 식별자(Vendor Identifier/VID)와 생산 식별자(Product Identifier/PID)를 활용하여 화이트 리스트를 작성하는 것입니다. 모든 USB 주변 장치의 한 가지 공통점은 PID는 출시되는 모든 신제품마다 다르지만 각각의 제조사는 고유한 VID를 지닌다는 것입니다.

화이트 리스트를 작성하기 위해, 제조사의 VID만 활용하는 것은 보안을 제공하기에는 너무 폭이 넓습니다. 해당 업체에서 제작한 USB 장치는 모두 허용될 수 있기 때문입니다. PID를 통해 이를 개선하고 호스트 시스템에 특정 모델의 액세스만을 요구합니다.

향상된 방법이지만, 아직은 이상적인 정도는 아닙니다. USB 저장 장치는 사용자들이 자신만의 장비에 권한을 지닌 전용 모델을 가질 수 있을 만큼 매우 널리 쓰입니다. 이런 점들을 중심으로 Kingstone Technology에서는 USB 저장 장치의 보안을 강화하는 맞춤형 솔루션을 제공합니다.

주문 제작 프로그램 덕에 특정 기관에 대한 맞춤형 PID 프로필은 다양한 Kingston 암호화 USB 플래시 드라이브에서 생성 및 적용될 수 있습니다. 전용 생산 식별자를 활용하여 장치를 사용하는 회사는 화이트 리스트 작성의 편이성에 따른 이점뿐만 아니라 크게 향상된 보안 능력도 갖출 수 있습니다. 전용 맞춤형 PID가 없으면, 직원들이 따로 구입해서 겉으로 똑같아 보이는 장치일지라도 액세스를 거부하게 됩니다.

맞춤형 PID를 사용하면 IT 운영자는 새로운 USB 저장 장치를 작업 과정에서 빠르고 쉽게 가져올 수 있을 것입니다.

그리고 또 다른 방법으로는 대부분의 Kingston 암호화 USB 드라이브가 제공하는 각 장치의 일련 번호를 사용하는 것이 있습니다. 이런 방식은 각 장치의 고유한 일련 번호가 엔드포인트 관리 제품군에 등록되어 있어야 합니다. 우선 IT 직원의 작업을 필요로 합니다. 그리고 Kingston에서 순서에 따라 일련 번호 목록을 제공합니다(목록은 항상 문자와 숫자로 비연속적으로 구성됩니다). 이 방법을 채택함으로써 각 드라이브 주인의식을 바탕으로 한 훨씬 유연한 정책이 가능해집니다. 또한 IT 포렌식 상황에서 아주 중요한 정확한 장비 출처 추적이 가능합니다. 몇몇 Kingston 드라이브는 전자 스캔을 위한 케이스에 바코드와 일련번호를 포함합니다. 또 비즈니스를 위해 케이스에 바코드와 일련 번호를 추가하도록 주문제작이 가능한 드라이브도 있습니다. 이러한 제품들은 장치 추적에 활용할 수 있습니다.

기본적으로, 엔드포인트 관리 시스템은 포트 차단과 화이트 리스트의 역할을 하며 VID/PID의 액세스를 제공합니다. Kingston은 USB 저장 장치 사용에 있어서 더욱 포용적이고 창의적인 정책을 펼 수 있도록 이러한 특성을 다루는 범용적인 방법을 제공합니다. 적절한 식별 방법 설정함으로써, 모든 포트 차단'이라는 규정과 같은 입장은 지나치게 단순한 동시에 불필요합니다.

## 원격 사용자를 위한 안전하게 따라하는 솔루션

보안에 있어서, 장치 화이트 리스트는 문제의 절반만 다루고 있습니다. 달리 표현하면 절반의 솔루션만을 제공합니다.

그 편이성과 단순함 때문에 마찰 없는 데이터 전송의 휴대성이 중요한 많은 비즈니스와 기관에게 USB 저장 장치는 없어서는 안 됩니다. 좋은 IT 위생을 준수하기 위해서 대부분의 환경에서 그러한 업무를 위해 암호화 USB 드라이브를 다루는 직원을 뽑는 것이 필수적입니다. 휴대용 저장 장치는 비밀번호 보호와 장치 암호화를 병용함으로써 장치 분실, 도난 등 잠재적으로 취약한 상황에서 민감한 데이터에 대한 액세스를 보호합니다.


암호화 기술은 다양하기 때문에 모든 상황에서 적용되는 솔루션은 아닙니다. 소프트웨어와 하드웨어 암호화 솔루션을 비교해보면 가장 큰 차이를 알 수 있습니다. 그렇다면 무엇이 최선일까요? 이는 귀하의 필요사항에 달려있지만 “무엇이 보다 안전할까요?”라고 묻는 것이 보다 성실한 질문이 될 것입니다.

소프트웨어 암호화는 기본적으로 더 적은 작용으로 일정 영역을 만족시키는 예산의 선택입니다. 데이터 전송에 민감하지 않고 규정 준수에 집중하는 비즈니스도 만족할 수 있을 것입니다.

하지만 소프트웨어 암호화의 작업 방식이 클라이언트를 대면하면서 컴퓨터 암호화 업무에 의존하는 어플리케이션을 요구하기 때문에 이것 역시 아킬레스건입니다. 둘이 연결되면서 소프트웨어 암호화 저장 장치는 호스트 컴퓨터에 따라 안전이 좌우됩니다.

컴퓨터 메모리에 액세스하는 해커들은 암호화/암호 해독 키를 “호시탐탐 노리므로” 침입에 대한 노출 또한 강조됩니다. 또 암호화 파일에 대한 액세스와 복사가 가능해지면 비밀번호 액세스 보호가 불필요해지면서 드라이브의 데이터는 무차별 공격의 대상이 될 수도 있습니다.

소프트웨어 기반 암호화는 IT 직원에게는 짐이 되겠지만 실행이 어려워지도록 주기적인 소프트웨어 업데이트가 필요하다는 것을 기억해야 합니다. 최악의 경우, 드라이브 장치 간의 전송에 미숙한 직원에 의해 소프트웨어 암호화 전부가 제거될 수도 있습니다. 드라이브 사용자는 암호화된 드라이브의 데이터를 컴퓨터에 복사하고, 드라이브를 암호화 이전 상태로 포맷한 뒤 해당 드라이브에 다시 데이터를 복사하는 일도 있을 수 있습니다. 이 때에 해당 데이터는 보호되지 못하고 위기에 그대로 노출될 것입니다. 데이터 개인 정보에 대한 법률 및 규정을 따른다면, USB 드라이브의 보안이 쉽게 무력화되는 것은 인정할 수 없습니다.

# 온칩 암호화: 강력하고 빠른 솔루션

반대로 하드웨어 암호화 USB 드라이브는 암호화를 관리하는 실제 드라이브에 포함된 전용 프로세서를 가지므로 컴퓨터와는 독립적으로 기능합니다. 그건 비밀번호 무차별 공격을 방어하는 상시 접속 암호화 프로세스를 지니고 있습니다. 암호화된 데이터는 액세스할 수 없고 복사되지 않습니다.

Kingston의 기업 및 군사용 암호화 하드웨어 USB 드라이브는 XTS 모드에서 AES 256 비트의 암호화를 사용합니다. AES 256 비트는 전세계적으로 사용되는 암호화 기술로서, 철저하게 데이터를 보호합니다. 각각 다른 등급의 암호화/해독 프로세스를 지닌 두 개의 키를 분리하여 사용함으로써, XTS 모드는 데이터를 두 번 암호화하는 것과 비슷한 효과를 지니게 됩니다.

사용 시 암호화 키는 사용자 비밀번호로 해제하는 드라이브 컨트롤러의 임의 숫자 생성기에서 생성됩니다. 복호화 하드웨어 내에서 인증이 이루어지기 때문에 암호화 키와 다른 중요한 보안 기능은 배드 USB와 콜드 부트 공격, 악의적 코드, 무차별 공격과 같은 일반적인 위협을 방어합니다.

하드웨어 암호화의 가장 즉각적인 이점 중 하나는 호스트 컴퓨터로 암호화 작업을 전송하지 않기 때문에 드라이브의 성능이 소프트웨어 암호화 드라이브 보다 확연히 좋다는 것입니다. 모든 것이 드라이브 내에서 이루어집니다.

Kingston IronKey D500S와 같은 하드웨어 암호화 USB 드라이버는 장치 외부에서 암호화된 비밀번호로 보호되는 장치입니다. 주암호화 저장 볼륨 해제와 비밀번호를 인증하는 어플리케이션을 포함하기 때문에 사용 시 쓰기 보호 런처 볼륨만이 시작되는 것을 볼 수 있습니다. 이 과정에서 호스트 PC에 어떤 종류의 드라이버나 소프트웨어도 설치되지 않습니다.

더욱이, Kingston의 하드웨어 암호화 USB 드라이브는 드라이브 내의 모든 종류의 펌웨어 조작을 방지하는 디지털 서명된 펌웨어입니다. 이렇게 보안을 한 층 높임으로써 USB 장치 펌웨어의 내재적 취약점을 위협하는 배드 USB와 같은 공격을 방어할 수 있습니다. 이건 호스트 컴퓨터에서 실행되고 있는 악의적 코드나 몰래 실행되는 명령을 초래할 수 있습니다.

물론, 모든 포트 차단'식 접근은 배드 USB의 위험은 제한할 것입니다. 하지만 그런 낡은 규정 탓에 생산성을 희생해야 할까요? 앞서 강조했듯, 하드웨어 암호화 USB 드라이브를 소개하는 간단한 조달과 배치 절차만 진행된다면 보안 환경은 휴대용 저장 장치 사용과 협력하여 유지됩니다.

# 원격 작업 준수와 보안

기관의 안전한 작업 환경의 보호로부터 떨어져서 원격 작업을 하는 분들은 우선순위의 재검토와 전략의 개선을 요구합니다.

원격 보안 계획에 있어서, 직원 노트북의 USB 포트를 차단하고 인터넷 접속으로만 서버에서 서류를 주고 받는다면 장점을 찾을 수 있을까요? 길 위의 와이파이 액세스 포인트처럼 보안과 신뢰도가 확실하지 않은 공개적인 인터넷 접속이 가능한 전부일 것입니다. 그리고 이런 행위는 위반의 가능성을 크게 높이는 광범위한 위험을 가져옵니다. 중간자(Man-In-the-Middle, MitM) 공격, 네트워크 도청, 스푸핑(위장)을 통한 감시 및 데이터

가로채기와 같은 위협은 사이버 범죄가 가능한 고도로 정교해지는 해킹 수법 중 일부일 뿐입니다. VPN 조차도 위태롭습니다.

기관의 네트워크가 인터넷에 연결된다는 것은 또다른 엔드포인트이고 네트워크의 내재된 노출로 인해 네트워크는 극도로 취약한 상태가 되어 진입 지점으로 표적화됩니다. 특히 민감한 데이터라면 원격 액세스를 통해 개방하는 것은 자체의 보안 위험을 동반합니다.

원격 작업자들에게 비밀번호 보호 하드웨어 암호화 USB 드라이브를 맡기는 것은 잠재적인 네트워크 취약점을 효율적으로 제거합니다. 하지만 그런 제공을 위해선 가능한 USB 드라이브와 그것들이 각 원격 작업자들의 환경에 어울리는 지에 대한 자세한 조사가 요구됩니다. 드라이브의 성능을 고르거나 시리얼 번호가 로그된 것을 선택할 지 정하는 것은 간단한 문제는 아닙니다. 여기에선 장치 자체가 제작되는 물리적 과정을 고려해야 합니다.

## 변조 방지 보호: 분명한 옵션들

여기서 주된 이슈는 하드웨어 암호화 USB 드라이브가 변조 방지인지 아닌지입니다. 이러한 간섭에 대한 장치의 보안 정도는 FIPS 140-3와 같은 기준에 반영되어 있는데 이 기준에는 암호화법을 사용하지 않고도 드라이브의 물리적 구성에 대한 탄력성을 면밀히 검토할 수 있는 몇몇 수준이 구성되어 있습니다.


관련 FIPS-197 인증은 데이터 보안 요구 사항이 군용 등급 수준이 아닌 엔터프라이즈 지향 모델인 IronKey Vault Privacy 50 시리즈 및 Vault Privacy 80 외장 SSD와 같은 하드웨어 암호화 속성 및 장치만 관찰합니다. 이런 드라이브는 저렴하지만 물리적 드라이브 변조를 방어할 수 없습니다.

FIPS 140-3의 3등급 인증(보류 중)은 장치 변조 노출을 위해 사용된 방식이 군사용 수준일 때 부여됩니다. Kingston 은 전 세계의 기업, 정부 및 군에 위 FIPS 140-3 3등급 드라이브를 공급합니다.

에폭시가 내부 드라이브 회로 전부에 코팅되며 내부 부품들과 케이스를 접착시키면서 추가 방어층과 보안을 형성합니다. 금속 케이스를 개봉하려는 시도는 매우 어려울 것입니다. 또 내부의 칩들과 기타 부품을 망가뜨려 드라이브가 기능하지 못하게 될 것입니다. 이런 단단하고 불투명한 에폭시가 첨가되면서 필수 부품의 변조는 불가능에 가까워집니다. Kingston IronKey D500S 및 S1000과 같은 장치에는 이 추가 보안 조치가 포함되어 있습니다.

이러한 장치 보호는 물리적 조치에만 한정되지 않습니다. Kingston IronKey S1000은 추가 등급의 변조 방지를 적용합니다. IronKey S1000의 내부 암호화칩은 모든 종류의 물리적 변조를 감지하고 장치가 켜짐과 동시에 드라이브를 사용할 수 없게 만듭니다. 민감한 파일을 액세스하고 전송하는 데 있어서 하드웨어 암호화 USB 저장 장치의 힘을 빌리는 것은 마찰 없는 원격 작동을 가능케 하고 현장 의 보안을 효과적으로 보증하는 실용적인 행동입니다.

USB 드라이브 하드웨어와 보안 특성을 조사하여 사용자의 특정 필요와 상황에 알맞은지 분명히 확인하십시오. 이런 결정에 있어서 믿을 수 있는 인증의 도움을 받아서 각 USB 드라이브는 반드시 케이스별로 살펴보아야 합니다. Kingston은 무엇을 우선사항으로 하든지 간에 저렴한 가격으로 모든 환경에서 사용할 수 있는 다양한 하드웨어 암호화 USB 드라이브 솔루션과 사용자 지정 옵션을 제공합니다. 일반적인 규정 준수에서 차원이 다른 군사용 성능까지 아우를 수 있습니다.

# 보안 우선: 네트워크가 없다면, 문제도 없습니다.

오늘날 사무실엔 국경도 없고, 재택 근무가 유행하고 있습니다. 이런 현상 탓에 수많은 회사에선 원격 액세스의 취약성이라는 이슈가 대두됐습니다. 많은 사람들은 이런 어려움을 처음으로 겪고 있습니다. 그리고 널리 퍼지는 이런 트렌드를 수용하기 위해 더 안전한 방법을 찾고 있습니다.

다양한 산업군에서 발생하는 이런 요구를 지원하기 위해서 하드웨어 암호화 USB 저장 장치는 여러 이유로 인해 네트워크를 이용한 데이터의 전송이 실용적이지도 바람직하지도 못한 곳에서 이미 자리를 잡고 보안 솔루션을 제공하고 있습니다.

재정 업무에 있어서, 규제 기관은 회사의 활동과 규정 준수에 대한 데이터 체크를 빈번히 요구합니다. 구체적인 투자 세부 사항과 교역, 기타 비밀 은행 업무를 포함하는 민감한 문서를 네트워크를 이용하여 전송하려고 할 때 노출의 위험은 훨씬 커집니다. 하드웨어 암호화 USB 드라이브의 정보를 제공해 드리기 위해 이 간단하고 효율적인 솔루션을 준비했습니다.

의료 환경에서 보안 USB 드라이브를 사용하여 파일을 전송하는 것은 일상에서 흔히 일어나는 일입니다. 파일을 분석하고 그것들을 연구에 참고하거나 의학도들에게 사례를 보여주길 원하는 의사나 상담가의 편이성을 위해서도 적용됩니다. 또 네트워크 액세스가 없거나 안전하지 않은 곳에서의 의료용 영상 장치 같은 전용 시스템에 대해서 더욱 실용적인 활용도 있습니다. 규정 준수 하드웨어 암호화 USB 드라이브를 활용하여, 파일들을 쉽게 전송하여 다른 곳에서 사용할 수 있습니다.

이 시나리오에서는 Kingston IronKey Keypad 200(KP200)이 그 진가를 발휘합니다. OS 독립형 드라이브이기 때문에 비밀번호를 입력해야 하는 런처 볼륨이 없습니다. 다만 모든 플랫폼에서 사용하기 위해 장치를 해제할 문자와 숫자가 혼합된 키패드가 필요합니다. 맥가이버 칼처럼 하드웨어 암호화 USB 드라이브의 활용도는 제조업에까지 미칩니다. IT 조사를 통해 얻은 안전 전송 어플리케이션과 운영 기술(OT) 플랫폼에 의한 기계 개발 분야 등 다양합니다. Linux를 포함해서 혼합 플랫폼 운영에서 KP200은 가능한 가장 간편한 보안 솔루션입니다.

하드웨어 암호화 USB 저장 장치에는 법률 집행 역할이라는 중요한 역할도 수행할 수 있습니다. 그들은 보호하고 이미지와 다른 증거들 같은 사건 파일을 현장 요원들이나 조사단, 포렌식팀에게 안전하게 전송합니다. Kingston은 드라이브 외부 케이스에 바코드와 함께 내부 시리얼 번호를 제공하기 때문에 추가적인 장점을 제공합니다. 드라이브의 실행과 분류과 간편해지고 추적이 용이해집니다. 시리얼 번호를 부여하는 것만큼 쉽고 바코드를 스캔하는 것만큼 빠릅니다. 회계 감사와 창고 관리는 더 없이 쉽습니다. Kingston IronKey D500S, D500SM 및 S1000B/E 드라이브 에서 기본적으로 보이는 특징입니다. 그렇지만 Kingston 주문 제작 프로그램의. 일환으로 다른 하드웨어 암호화 모델에서도 가능합니다.

## 해야 할 것과 하지 말아야 할 것

✓ **규정을 준수하면서 안전한 드라이브를 사용하십시오.** 그리고 사용처의 필요에 알맞는 드라이브를 얻으려면 성능을 확인하십시오.

✗ **결코 개인장비활용(BYOD) 규정이나 임의로 권한을 부여하지 마십시오** – 암호화되지 않은 드라이브를 분실하는 회사는 재정적으로 지속적으로 막대한 비용과 피해를 감수하게 됩니다.

✓ **엔트포인트 관리 제품을 이용하십시오.** 그리고 탁월한 화이트 리스트 기능을 제공하는 하드웨어 암호화 USB 드라이브를 사용하십시오.

✗ **어떤 것도 우연에 맡기지 마십시오.** 사내 혹은 원격 작업 환경에 필요한 요구 사항을 적절히 평가하십시오.

✓ 보안 문제에 대해 **직원들을 교육하십시오.** 회사의 보안이 위협으로부터 유지될지는 개인의 관심에 달려있습니다.

✗ **결코 보안을 너무 복잡하게 만들지 마십시오.** 사용자가 사용되는 IT 솔루션을 저해하는 해결책을 찾을 수 있습니다. 규정과 정책이 지금까지 적용되어 왔다고 해서 모든 상황에 어울리는 것은 아닙니다. 작업 환경은 변화하고 있고 올바른 솔루션과 새로운 정책을 선택함으로써 개선되고 강화될 수 있습니다.

# 보안과 저장 이동성: 최첨단 기술

비밀번호 보호, 하드웨어 암호화, 변조 방지 보호, 엔드포인트 화이트 리스트, 군사용 FIPS 140-3 3등급 인증(보류 중) 및 즉각적인 로깅은 Kingston USB 드라이브의 지체 없이 출고가 가능한 기술입니다.

이런 강력한 보안 방어는 USB 드라이브와 그 데이터가 호스 환경에서 확실히 안전하게 보호합니다. 글자 속 성능은 훌륭하지만, 아무런 조사 없이 무작위로 모델을 선택하게 되면 일부 기관에선 요구 사항에 이상적으로 부합하지 않을 수 있습니다.

독립적인 제조사로서, Kingston은 고객의 요구를 만족시킬 폭 넓은 옵션을 제공합니다. Kingston의 주문제작 프로그램을 통해 매끄러운 사용자 경험을 제공하기 위해 성계된 진보된 솔루션이 가능합니다.

보안 주문제작은 기관에 화이트 리스트를 위한 자체 USB PID를 공급하는 것 그 이상입니다. 런처 애플리케이션의 보안 프로파일은 연락처와 회사의 자세한 사항에서 비밀번호 힌트의 활성화와 최대 비밀번호 시도 횟수 결정에 이르기까지 15가지의 다양한 기본설정을 사용하여 사용자가 설정할 수 있습니다. 외부엔 특정한 드라이브는 다양한 색은 물론 회사 브랜드(로고)를 입력할 수 있습니다. 드라이브 최소 주문 수량인 50개로도 위의 모든 특성은 장치 사용에 있어서 손쉬운 통합을 제공합니다.

만약 USB 저장을 보호하는데 적합한 엔드포인트 관리 어플리케이션이 없다면, 원격으로 비밀번호를 초기화할 수 있는 옵션을 가진 Kingston 장치를 관리하길 원하는 기관들이 사용할 수 있는 관리 솔루션도 있습니다.

USB의 유행과 편이성 덕분에 다양하고 유망한 기술들보다도 오래 살아남을 수 있었습니다. 그리고 USB 저장의 즉각성과 편이성을 활요하는 많은 업무를 가능하게 했습니다. 바로 사용가능하고 항상 안전한 보호 USB 드라이브는 바로 적용될 수 있는 간단한 솔루션을 제공합니다.

원격 환경에서 왜 네트워크 데이터 위협을 걱정할까요? Kingston IronKey 하드웨어 암호화 USB 저장 장치를 사용한다면, 해답은 귀하의 손 안에 있습니다.

알아보려면 kingston.com/ironkey를 방문하거나 보다 구체적인 질문이 있으면 당사의 암호화된 USB 전문가에게 문의하십시오.

**#KingstonIsWithYou #KingstonIronkey**