Kingston TECHNOLOGY

Matrix42와 제휴하여 설명하고, 탐색한 최적의 엔드포인트 보안

MATRIX42

#KingstonIsWithYou

Matrix42와 제휴하여 설명하고, 탐색한 최적의 엔드포인트 보안

소개

데이터 보호는 오늘날 세계에서 기업, 정부, 개개인이 우려하는 기본적인 요건입니다.

데이터 위반, 해킹, 인간 요소는 전 세계에서 계속 위협과 위험의 경종을 계속 울리고 있습니다. 데이터 위반 및 불운한 노출과 관련된 대가는 천문학적일 수 있습니다. 고급 사이버보안 및 엔드포인트 DLP 전략 요건은 모두 종속적이고 효율적인 스토리지 및 메모리에 따라 달라집니다.

모범 사례, 표준, 정책과 결합된 메모리와 고속 스토리지, 암호화의 사용은 중요한 단계입니다. 손상된 노트북 및 USB 드라이브는 개개인 및 회사가 개인 및 사설 정보 노출에 취약하게 만듭니다. Kingston은 기존 또는 개발 중인 보안 계획을 보완하면서 위험을 완화하기 위해 위협 예방 솔루션을 제공합니다.

Matrix42와 제휴하여 설명하고, 탐색한 최적의 엔드포인트 보안

컨텐츠

이 짧은 e북은 엔드포인트 솔루션, Kingston의 암호화 USB 드라이브, 주문 제작 프로그램과 Matrix42 EgoSecure Data Protection 소프트웨어가 어디에서 여섯 가지 부문 과제를 해결하는 데 도움이 되는지 살펴보고, 비즈니스 요구사항을 충족하는 솔루션을 살펴볼 것입니다.

우리는 이와 같은 여섯 가지 부문과 엔드포인트 보안 과제를 처리하는 방법에 대해 철저하게 분석하였습니다.

목차

섹션 1: 산업 사용 사례
정부 부문

상황:

정부 부문 내에서, USB 장치의 사용은 매우 일반적입니다. 예를 들어, 경찰서는 디지털 카메라로 찍은 주차 위반 및 행정 위반 사진을 USB 케이블을 통해 관계기관의 시스템으로 복사해야 해야 합니다. 경찰청은 외부 데이터 스토리지 장치로 수사 데이터를 받습니다. 이러한 데이터는 다시 쓰기할 필요가 있으며, 무단 액세스는 반드시 방지해야 합니다.

과제:

USB 드라이브에 대한 높은 수요로 인하여, 직원은 USB 드라이브를 정기적으로 요청합니다. 보안 이유로 개인 및 무단 데이터 스토리지 장치의 사용은 반드시 차단해야 합니다. 직원이 새로운 USB 스토리지 장치를 필요로 하면, 직원이 일에 방해를 받지 않도록 사용자 헬프 데스크를 통해 가능한 빨리 이용할 수 있어야 합니다. 적절한 USB 장치를 사용할 때 보안 문제가 발생하지 않는다는 사실에 주목하여야 합니다.

솔루션:

장치 제어, 데이터 필터링과 암호화를 결합할 때, 다음의 시나리오가 가능합니다:

일반적으로 알지 못하는 장치는 컴퓨터 엔드포인트에서 차단됩니다. 디지털 카메라와 같은 데이터 스토리지 장치는 이미지 파일 읽기와 같은 특정한 기능만 허용됩니다. 쓰기 작업은 일반적으로 암호화되고, 공인 USB 장치만 허용됩니다. 모든 데이터 액세스는 기록됩니다. 일련 번호와 하드웨어 ID를 주문 제작하여 승인 장치의 관리를 간소화할 수 있습니다. 따라서 Matrix42 Service Management는 Self-Service Portal에서 사용자가 맞춤화된 Kingston Technology USB 드라이브를 요청할 수 있도록 허용합니다. 승인 프로세스 이후, EgoSecure Data Protection에서 USB 장치의 사용이 자동으로 허용됩니다.

> “우리 직원은 짧은 승인 프로세스 이후 새로운 USB 장치를 쉽고, 빠르게 공급받을 수 있다는 사실에 흥분하고 있습니다. 우리는 Kingston Technology의 주문 제작 프로그램 Matrix42를 통한 쉬운 서비스 관리와 엔드포인트 보안에 매우 만족하고 있습니다.”
>
> **헬프데스크의 대표자, 정부 부문**

섹션 2: 산업 사용 사례
의료

상황:

외부 스토리지 장치는 직원과 다른 기관과 데이터를 교환하는 수단으로 여전히 자주 사용되고 있습니다.

예를 들어, 독일 병원은 암 등록부와 함께 현재 암 사례와 진행에 관한 정보를 반드시 제공해야 합니다. 용이함을 위해 모바일 데이터 스토리지 장치를 통하여 이러한 데이터를 전송할 때가 자주 있습니다.

의사 역시 각 강의에서 USB 드라이브를 통해 연구 데이터와 같은 문서를 가져올 것입니다.

과제:

환자 데이터는 매우 민감하며, 승인되지 않은 사람의 수중에 있어서는 안 됩니다. 따라서 데이터 보호를 높이고, 강화할 필요가 있습니다. 데이터 캐리어를 분실하는 경우, GDPR에 대해서는 문제 환자의 웰빙에 있어서도 중대한 문제가 될 수 있습니다. 이러한 이유로 인하여 USB 데이터 스토리지로의 액세서를 제어하고, 모니터링하고, 암호화하는 것이 중요합니다.

솔루션:

EgoSecure Data Protection는 하나의 솔루션에서 액세스 제어, 데이터 감사, 필터링 암호화와 같은 다양한 보호 조치를 결합하였습니다. IT 관리자는 직원에게 어떠한 장치에 대한 액세스 권한을 부여할 것인지 결정할 수 있습니다. 예를 들어, 일련 번호와 하드웨어 ID가 예외가 될 수 있습니다. 이러한 식별자는 Kingston Technology의 주문 제작 프로그램 덕분에 정의가 가능하며, 따라서 기업이 승인한 장치만을 사용할 수 있도록 Data Protection 관리에서 오직 하나의 값만 구서할 필요가 있습니다. 그 결과 관리 노력은 매우 줄어들고, 액세스가 암호화되고 모니터링 되어 데이터 보안(GDPR, CCPA, HIPAA 등)은 증가합니다.

> “우리는 이미 Kingston 암호화 USB 드라이브를 사용하고 있습니다. 지금 EgoSecure Data Protection을 통해 우리는 환자 데이터 전송 추적성이 EU-GDPR에 따라 실현되었다는 사실을 보장할 수 있습니다.”
>
> **CISO, 대학병원**

섹션 3: 산업 사용 사례 재정

상황:

은행은 다양한 규정 준수 요건이 적용됩니다. 이러한 요건 중 하나는 PCI-DSS(결제카드산업정보보안표준) 규정 준수입니다. PCI-DSS 요건에 데이터 암호화, 취약성 분석과 데이터 필터링 필요성이 포함됩니다. 목적은 위협과 IT 보안 위험을 최소화하거나 완전히 방지하는 것입니다.

과제:

IT 보안 면에서 엔드포인트에 여러 위험이 있습니다. 고용인은 매일 소비자와 기업의 결제카드 정보를 취급하고, 금융 기관의 민감 데이터를 처리해야 하며, 따라서 클라우드, 이메일, USB와 웹 데이터가 악성 프로그램에 의해 손상될 위협이나 적절하게 보호하지 않을 경우 데이터가 실수로 제 3자의 수중에 들어갈 위협에 노출됩니다. 그러한 사고는 GDPR, PCI-DSS 면에 있어서는 물론 Sarbanes-oxley 법안에 있어서도 은행에 재무적인 영향을 미치는 위험이 될 것입니다. 또한 사이버 범죄자들은 다양한 방법으로 은행 시스템에 영향을 미치거나 조작하려고 시도하며, 이러한 과정에서 더욱 창의적입니다. 예를 들어 최근 돈을 훔치기 위해 전원 공급을 중단하고, 부팅 가능한 USB 장치로 시스템을 시작한 ATM 관련 사이버 범죄가 있었습니다.

솔루션:

IT 시스템은 다층 보호 조치로 보호해야 합니다. PreBoot Authentication을 통한 애플리케이션 제어, 이상 감지, UEBA(사용자 및 단체 행태 분석), 모니터링과 전체 디스크 암호화를 통해 이를 달성할 수 있습니다. Matrix42는 이를 자동, 통합 시스템에서 구현하였으며, 따라서 승인 애플리케이션과 암호화 USB 장치만 허용됩니다. 또한 의심이 되는 활동이나 악의적인 활동을 감지하고, 추가 조치를 자동으로 시작합니다. USB 드라이브의 사용과 관련해, Kingston Technology 주문 제작 USB 드라이브의 결합은 최소한의 노력으로 장치가 허용 목록에 포함되고, 추적 가능한 방식으로 데이터를 암호화했음을 확인하는 데 도움이 되었습니다. 추가적인 노력 없이 규정 준수를 상당히 높였습니다.

> “EgoSecure Data Protection와 화이트리스트 기능을 통하여, Kingston 함호화 USB 드라이브만 승인을 받을 수 있었습니다. 우리는 맞춤화 하드웨어 ID가 포함된 Kingston 암호화 USB 드라이브를 허용 목록에 포함시키는 한편 다른 장치는 허용하지 않았습니다. 이로 인해 관리 노력을 상당히 줄이면서도 보안은 높였습니다!”
>
> IT 관리자, 금융 기업

섹션 4: 산업 사용 사례
자동차

상황:

자동차 산업에서, USB 장치가 다양한 분야에 나타납니다. 예를 들어, 연구 데이터는 외부 스토리지 장치에 저장이 되고 기업의 각 엔지니어 사이에서 교환됩니다. 생산 기계를 구성할 때, 파일은 IT 환경에서 OT 환경으로 전송됩니다. 이러한 데이터 모두 매우 민감하며 산업 스파이와 데이터 도난으로부터 보호되어야 하며, 그렇지 않으면 쌓아 놓은 노하우가 잘못된 사람의 손에 들어갈 수 있습니다.

과제:

자동차 산업은 TISAX, 프로토타입 보호, ENX, ISO27001, “제 3자 연결” 및 GDPR과 같은 규정 준수 요건이 적용됩니다. TISAX에서 Control 9.1, 9.5, 10.1규약은 데이터 접근을 반드시 제어, 모니터링, 필터링 및 암호화해야 한다고 정합니다. 자동차 기업의 모든 영역에서 이러한 조치는 GDPR, ISO27001과 같은 다른 규정 준수 요건에서 준수해야 합니다.

솔루션:

Kingston Technology은 하드웨어-기반 암호화를 통하여 USB 드라이브 보안 데이터를 암호화하였습니다. 이러한 장치는 EgoSecure Data Protection에서 사용 가능하고, 데이터의 사용과 관련해서는 자동으로 허용 목록에 포함되는 맞춤 일련 번호와 하드웨어 ID를 가질 수 있습니다. 또한, 의심스런 활동이 있을 경우 데이터 이동을 모니터링하고, 분석할 수 있습니다.

> “Matrix42와 Kingston Technology을 통해, 우리는 사용자의 행태를 크게 바꾸지 않고 Control 9.5(정보 및 애플리케이션으로 액세스), Control 10.1(암호화)과 같은 TISAX 요건을 구현할 수 있었습니다.”
>
> **CTO, 자동차 공급자**

섹션 5: 산업 사용 사례
통신

상황:

통신 공급자는 소비자와 관련해 많은 정보를 갖고 있습니다. 이러한 정보는 매우 민감하며, GDPR에 대해 특히 그러합니다. 따라서 데이터 손실 및 데이터 도난을 방지하기 위해서는 충분한 조치를 취할 필요가 있습니다.

과제:

통신 기업 고용인은 매일 소비자 데이터를 취급합니다. 이러한 데이터 대부분은 비즈니스 애플리케이션 안에 저장됩니다. 그러나 소비자 계약이나 데이터베이스 보내기도 엔드포인트에 저장되고 외부 장치에 연결될 수 있는 위험이 있습니다. 데이터 교환에서, 사용자는 외부 스토리지를 자주 이용합니다. 따라서 정확하지 않은 데이터 스토리지 활동을 감지, 교정하거나 보호하는 것이 매우 중요합니다.

솔루션:

조달 프로세스를 간소화하기 위해, 주문 제작 제품 ID가 포함된 Kingston Technology 암호화 USB 드라이브를 EgoSecure Data Protection의 사전 정의 허용 목록에서 빠르게 구입하고, Matrix42 Service Catalog를 통해 배송하는 것이 가능합니다. 민감한 정보가 포함된 데이터 스토리지와 보내기는 “사용 데이터”와 “고정 데이터” 스캔을 기초로 한 딥-콘텐트 검사를 통해 자동으로 식별하고, 교정하는 것이 가능합니다. 데이터 이동이 중앙에서 기록됩니다. 따라서 직원은 요청과 승인 이후 바로 데이터 스토리지에 필요한 새로운 하드웨어를 빠르게 받을 수 있습니다. 이를 통해 GDPR 부합일 것임을 보장할 수 있습니다.

> “Matrix42의 self-servcie portal 덕분에 사용자는 필요한 스토리지 매체를 요청할 수 있습니다. 주문을 승인, 배송하였을 때, EgoSecure 장치 제어가 장치를 허용합니다. Matrix42와 Kingston Technology의 조합은 기업의 생산성과 보안을 높입니다.”
>
> **CTO, 통신 공급자**

섹션 6: 산업 사용 사례
제조 산업

상황:

미래에 황금은 디지털 데이터입니다. 제조 산업에서 이러헥 가치있는 데이터에 생산 계획, 소비자와 공급자에 관한 데이터, 기업 노하우가 포함됩니다. 데이터가 손실되면 GDPR 관점에서 심각한 불이익이 될 뿐 아니라, 기하급수적인 문제가 되고 명성에도 문제가 될 수 있습니다. 불행히도 USB는 택시, 세탁소, 공항, 기차역이나 주차장에서 매일 발견됩니다.

과제:

스토리지 장비에 매우 민감한 데이터가 포함되며 불행히도 이러한 데이터가 암호화되지 않는 경우가 자주 있습니다. 서비스 기술자는 생산 기계의 업데이트를 설치할 때 외부 데이터 캐리어를 사용하는 위험도 있습니다. 이러한 외부 장치는 네트워크에 악성 프로그램을 침투시킬 위험이 있습니다.

솔루션:

Kingston Technology은 하드웨어-기반 암호화를 통하여 USB 드라이브 보안 데이터를 암호화하였습니다. 이러한 장치는 EgoSecure Data Protection에서 사용 가능하고, 데이터의 사용과 관련해서는 자동으로 허용 목록에 포함되는 맞춤 일련 번호와 하드웨어 ID를 가질 수 있습니다. 또한, 의심스런 활동이 있을 경우 데이터 이동을 모니터링하고, 분석할 수 있습니다.

> “우리가 스스로 데이터 도난을 보호하는 데 있어 생산 데이터의 암호화가 매우 중요합니다. 이렇게 민감한 데이터는 EgoSecure Data Protection을 통한 승인 Kingston 암호화 USB 드라이브에서만 허용됩니다. 다른 모든 USB 장치에서, 생산 데이터는 차단이 되며, 외부 데이터 스토리지에 대한 쓰기 액세스는 EgoSecure의 on-th-fly 암호화와 로깅을 통해 보호됩니다.”
>
> **IT 보안 담당자, 제조 산업**

섹션 7: Kingston과 Matrix42의 솔루션

모범 사례, 표준, 정책과 결합된 메모리와 고속 스토리지, 암호화의 사용은 중요한 단계입니다. 손상된 노트북 및 USB 드라이브는 개개인 및 회사가 개인 및 사설 정보 노출에 취약하게 만듭니다. Kingston은 기존 또는 개발 중인 보안 계획을 보완하면서 위험을 완화하기 위해 위협 예방 솔루션을 제공합니다.

암호화 USB 드라이브 - Kingston Technology

Kingston의 하드웨어 기반 암호화 USB 플래시 드라이브는 조직 방화벽 내외부의 모바일 데이터를 위한 데이터 보호 솔루션을 특징으로 합니다. 완벽한 보안을 필요로 하는 데이터를 보호하도록 설계된 이 드라이브는 특정 산업 표준, 지침 및 규정을 충족하도록 도움을 줍니다. 제품은 TAA를 준수하고 FIPS를 인증 받았으며, 최대 용량은 128GB로 기업 사용자부터 정부 기관까지 모두에게 적합합니다.

안전한 주문 제작 프로그램

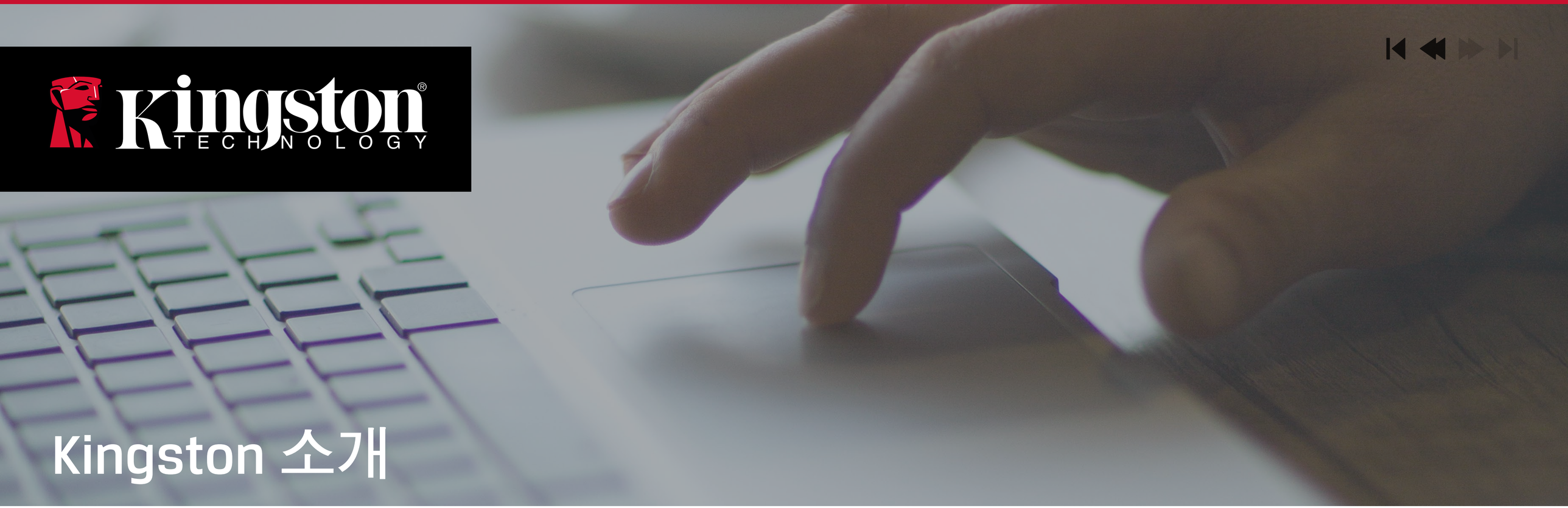
이제 Kingston의 암호화 USB 플래시 드라이브를 맞춤화하여 다양한 방법으로 귀사의 요구를 충족시킬 수 있습니다. 엄선된 기능을 추가하여 유일무이하고 없어서는 안 될 드라이브를 만들 수 있습니다. Kingston®은 당신이 선호하는 재판매 업체를 통해 USB 플래시 드라이브를 사용자 지정할 수 있도록 쉽고 편안한 주문 방식을 제공합니다. Kingston의 암호화 USB 제품군에는 DTVP30, DTVP30AV, DT4000G2, IKD300S 시리즈가 있습니다. 이 프로그램은 일련 번호, 이중 비밀번호 및 고객 로고 등 고객이 가장 자주 요청하는 옵션을 제공합니다. 최소 주문 수량은 50개, 재주문 수량은 25개로 구성된 프로그램은 조직이 필요로 하는 것을 정확하게 제공합니다.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection은 장치, 시스템, 데이터의 예방과 보호를 위해 기업에 360° 보안 관리를 제공합니다. 솔루션은 손상이 발생하였을 때 생산성 손실 없이 보호조치를 취할 수 있도록 전체 프로세스에서 예방과 감지를 자동화합니다.

요약

데이터 보호 및 사이버 보호는 엄청난 책임으로 느껴질 수 있습니다 직원이 언제, 어디서, 어떠한 장치로 작업을 할 것인지 결정할 수 있는 능력을 갖게 되면서 디지털 업무의 요건은 크게 바뀌었습니다. 하드웨어-기반 암호화 USB 드라이브와 엔드포인트 소프트웨어 관리의 올바른 좋바은 조직이 조직의 장치를 제어하는데 도움이 될 것입니다. 따라서 데이터 위반 위험을 줄이고, GDPR 규정 준수 전략을 계속해서 지원합니다.



Kingston 소개

30년이 넘는 경험을 가진 Kingston Technology는 조직에 문제를 발생시키지 않고 엔드포인트 보안 과제를 식별, 해결하는데 필요한 지식을 보유하고 있습니다.

#KingstonIsWithYou