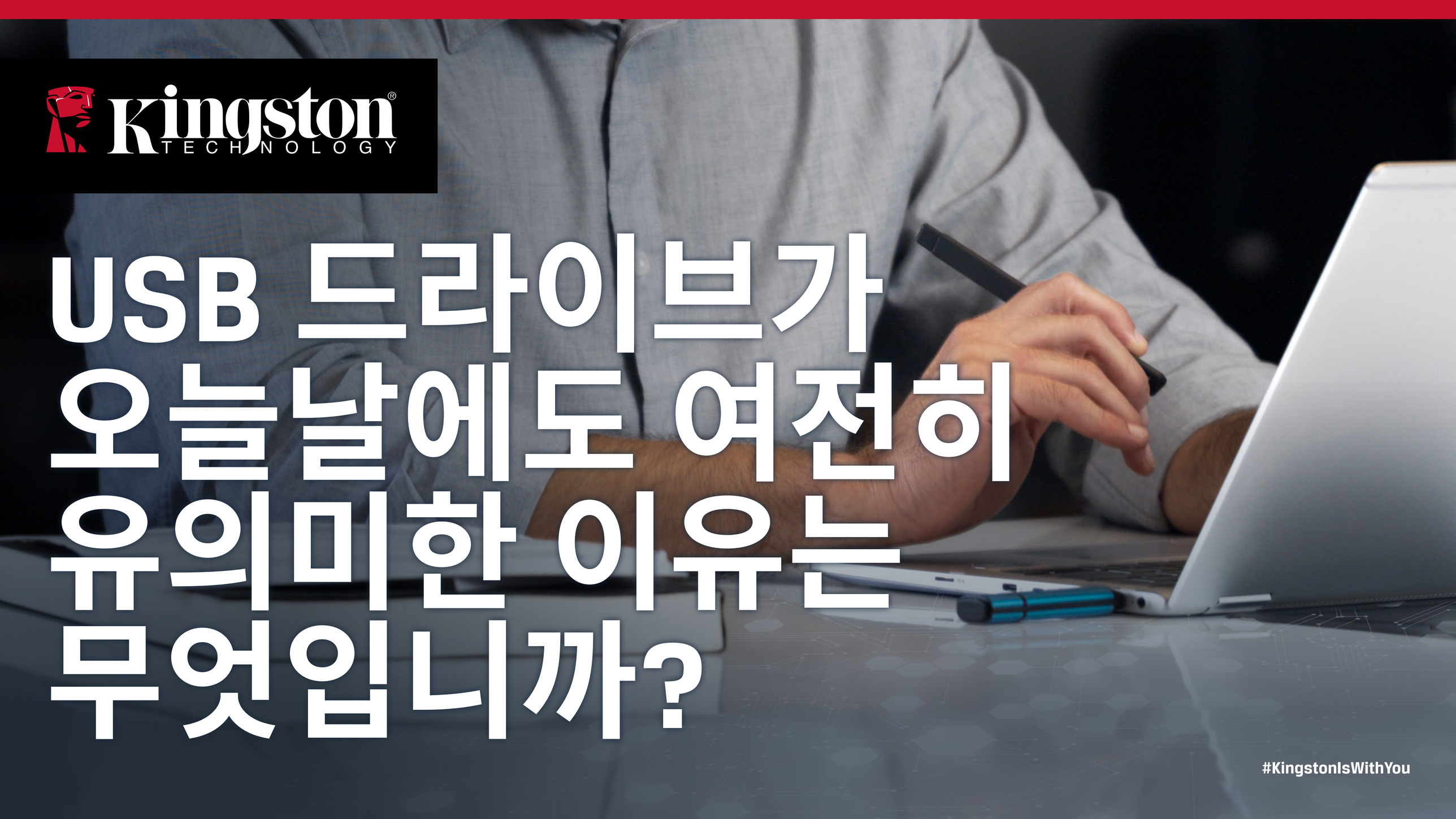

Kingston
TECHNOLOGY
USB 드라이브가
오늘날에도 여전히
유의미한 이유는
무엇입니까?
#KingstonIsWithYou

USB 드라이브가 오늘날에도 여전히 유의미한 이유는 무엇입니까?

서문 및 목차

전 세계 모든 기업 데이터의 60%가 클라우드[1]에 저장되는 오늘날의 디지털 시대에, 30년 가까이 된 스토리지 기술의 의의를 논의하는 것은 다소 기묘하게 느껴질 수도 있습니다. 그러나 도입 이후로 이 스토리지 필수품은 쭉 진화해 왔으며 계속 발전하고 있습니다.

USB 드라이브가 단지 파일, 드라이브 및 애플리케이션을 연결하는 표준 수단이었던 시대는 이제 지났습니다. 오늘날의 솔루션은 대단히 향상된 전송 속도를 자랑할 뿐만 아니라 많은 상황에서 필수인, 신뢰할 수 있으며 안전한 휴대용 미디어를 제공합니다. 그러나 클라우드 스토리지 솔루션이 겉보기에는 같은 이점들을 많이 제공할 수 있는데 USB 드라이브가 어떻게 여전히 의미가 있을까요?

이 eBook에서는 클라우드가 지배하는 환경 속에서 USB 플래시 드라이브가 자리하는 위치에 대해 논의할 것입니다. 주요 업계 전문가 몇 사람의 주요 통찰력을 바탕으로 오늘날의 조직에서 USB 드라이브를 사용하는 방법을 살펴보고 이러한 USB 드라이브가 소프트웨어 기반 암호화, 독립적인 스토리지 환경 및 엔드포인트 데이터 보안 가운데 자리하는 그 위치에 대해 논의합니다.

USB 드라이브가 오늘날에도 여전히 유의미한 이유는 무엇입니까?

기고자

이 eBook은 IT 및 첨단 기술의 업계 전문가 3명이 함께 만든 것입니다.

Rafael Bloom

Rafael은 기술 제품, 마케팅 커뮤니케이션 및 사업 개발 분야의 임원으로 오랫동안 근무해 왔습니다. Rafael은 기술과 규제의 변화로 인해 발생하는 조직, 제품 및 의사소통 관련 문제들에 대해 집중적으로 조언합니다. 이렇게 고도로 다양한 분야에는 의도적인 정보 거버넌스 및 규정 준수, 데이터 보호 및 첨단 기술(예: AdTech, 모바일 및 5G, AI 및 머신러닝)에 정통한 직무 전문가가 필요합니다.

Tomasz Surdyk

Tomasz는 24년 넘게 각국 정부의 IT 보안 부서를 두루 거친 정보 보안, 개인 데이터 및 사이버보안 분야의 업계 유명 인사입니다. 그는 이전에 행정자치부에서 기밀 정보와 개인 데이터를 처리하는 ICT 시스템과 네트워크를 조사했으며, NATO 및 EU에 보안 승인을 받았습니다. 또한 몇 년간 비즈니스 정보와 개인 데이터의 보안을 강화하는 보안 솔루션을 구현하는 전문 기업의 소유주이기도 했습니다.

David Clarke

David는 Thompson Reuter가 선정한 “영국의 소셜 미디어, 위험 관리, 규정 준수 및 레그테크 분야에서 가장 영향력 있는 이론가 및 사상가 30명” 중 최고 영향력 있는 10명으로 인정받고 있으며, Kingston Technology의 최고 글로벌 전문가 50명에 선정되었습니다. David는 과거에 글로벌 FTSE 100개 기업에서 보안서비스제공 담당 글로벌 책임자 및 보안 인프라 책임자 등 다수의 보안 관리 직책을 두루 거쳤습니다.

USB 플래시 드라이브의 부상

20여 년 전 최초의 USB(Universal Serial Bus) 드라이브가 시장에 등장했을 당시 이 드라이브의 공동 호환성은 컴퓨터 기술 분야의 판도를 바꾸어 놓았습니다. 대중이 여러 장치 작업에 광범위하게 액세스할 수 있는 기능을 갖춘 USB는 2000년 최초의 USB 플래시 드라이브 출시와 함께 즉시 진화하여 훨씬 더 빠른 데이터 전송, USB 3.0 포트 및 훨씬 더 뛰어난 기능을 제공했습니다.

그 이후로 모바일 데이터 스토리지 및 보안 요구사항 측면에서 기술은 크게 발전했습니다. 중요하게 살펴보아야 할 것은 매우 특정한 사용 사례를 염두에 두고 설계된 오늘날의 USB 드라이브 세대입니다. 기업 관점에서 본다면, 원격 및 하이브리드 작업의 증가, 클라우드 서비스 이용, 그리고 사이버 보안 문제로 인해 보다 효과적인 솔루션이 필요합니다. 이에 따라 규제 요건은 데이터를 규정에 준수하여 저장할 것을 요구합니다. 이러한 압력은 으레 "온프레미스(on-premise)"로, 그리고 클라우드에서 실행될 수 있는 분산적이고 복잡한 시스템으로 인해 한층 가중됩니다.

그리고 정형 및 비정형 데이터(문서, 이메일, 사진, 비디오, 메타데이터 등)의 양이 증가하는 문제가 있으며, 이 모든 문제가 갈수록 진화하는 기업용 스토리지 요구사항을 한층 복잡하게 만들고 있습니다.

그러나 클라우드 스토리지가 이러한 많은 문제들을 해결할 수 있다면, USB 드라이브가 오늘날의 비즈니스 환경에서 가지는 의의는 무엇입니까?

> "USB 드라이브는 과거에 거의 일회용, 저성능, 보안 수준이 낮은 장치로 사용되었기 때문에 많은 사람들이 이러한 USB 드라이브를 구식이거나 보잘것없다고 생각합니다."
> - Rafael Bloom

변해가는 수요를 충족하는 휴대용 스토리지

USB 드라이브를 휴대용 스토리지로 사용하는 오랜 경향이 사라져 가는 동안 고성능 USB 드라이브가 등장하여 데이터 보호 및 기밀성이 추가된 개인적이고 안전한 로컬 백업에 사용되었습니다. 이는 HR 기록, 금융 데이터, 의료 서비스 기록, 지적 재산(IP) 보호, 모든 개인 식별 정보(PII) 등 규정 준수에 민감한 데이터의 경우 매우 중요할 수 있습니다. 또한 이 세대의 장치는 다음과 같은 용도로 사용할 수 있는 빠른 데이터 전송, 저장, 백업 및 보안 기능이 제공됩니다.

- 직접 전달해야 하는 규정 관련 정보
- 현장 또는 오프사이트에서 전달 및 인쇄해야 하는 법률 및 재무 문서
- 랜섬웨어가 위협이 될 수 있는 적대적인 가능성을 지닌 모든 환경
- 네트워크 액세스가 허용되지 않는 인쇄 시스템으로의 전송

주요 암호화 USB 제공업체 Kingston Technology는 Kingston IronKey™ S1000과 같은 솔루션을 출시하는 등 변해가는 수요에 발맞추어 변화했습니다. 이 동급 최고의 암호화 USB 드라이브는 강력한 안티탬퍼링(anti-tampering) 보호 기능이 있는 별도의 암호화칩(cryptochip)과 함께 XTS-AES 256비트 암호화를 제공함으로써 기밀 데이터를 보호하는 기능을 갖추어 가장 엄격한 기준을 충족하고 있습니다. 더불어, FIPS 140-2 Level 3 인증 또한 받았습니다. 이는 암호화 하드웨어로서의 그 효율성을 미국 정부가 공식적으로 검증했음을 의미하므로 데이터 보호 면에서 제품의 신뢰성이 중요한 조직에 이상적인 솔루션입니다.

이러한 하드웨어 암호화 USB 드라이브는 데이터가 클라우드 기반이든 온프레미스 방식이든 관계없이 중앙 집중식 보안 장치 관리 솔루션을 제공합니다. 또한 규정을 준수하는 암호화 데이터 스토리지는 소프트웨어가 필요 없을 만큼 사용하기 용이하므로, 귀중한 IT 시간을 확보하여 빠르고 효율적인 배포를 위해 설계된 솔루션을 제공합니다.

변해가는 수요를 충족하는 휴대용 스토리지

백업 및 보관은 USB 드라이브를 사용하여 장기적으로, 그리고 타사 클라우드 서비스와 별개로, 디지털 자산을 보호할 수 있는 또 다른 예입니다. 클라우드에서 대용량 데이터 전송을 쉽게 처리할 수 있는 것은 사실이지만 독점 IP는 여전히 민감할 수 있으므로, 암호화된 보안 USB 드라이브에 저장할 가치가 충분하며, 이를 통해 인터넷으로부터 멀리 떨어져 안전하게 보관할 수 있습니다.

그러면 특히 암호화 드라이브를 사용하는 경우, 조직에서 논리적, 물리적으로 데이터를 통제해야 하는 상황이 항상 있을 것입니다. 그리고 HDD/SSD의 스토리지를 암호화할 수 없는 경우들도 있습니다. Kingston IronKey D300S와 같은 외장 암호화 USB 드라이브를 사용하면 이 문제를 해결할 수 있습니다. 이 USB 플래시 드라이브는 128비트 데이터 블록을 암호화할 수 있는 블록 암호 유형인 XTS 256비트 AES(Advanced Encryption Standard, 고급 암호 표준) 하드웨어 암호화 기능을 갖추고 있습니다. 그리고 이보다 더 많은 데이터를 암호화해야 하는 경우, AES는 이전 모드보다 더욱 우수하고 강력한 데이터 보호를 제공할 수 있는 XTS 블록 암호 모드를 사용합니다.

> 제가 볼 때, USB 플래시 드라이브는 여전히 사용되고 있으며 데이터 보안에 필수적인 부분입니다. 이 드라이브는 적절한 스토리지 및 보호는 물론 장치 간에 정보를 신속하게 전송하는 데에도 사용됩니다.
> - Tomasz Surdyk

암호화: 하드웨어 기반과 소프트웨어 기반 비교

데이터가 암호화되는 방식을 살펴볼 때, 하드웨어 암호화 쪽이 소프트웨어 암호화보다 관리하기 쉽고 안전하다고 주장할 수 있습니다. 암호화 프로세스가 호스트 시스템의 나머지 부분과 별도로 유지되어 가로채거나 손상시키기가 훨씬 더 어렵기 때문입니다. 중앙화된 장치 수준의 관리는 LAN 및 인터넷 연결 전반에 걸쳐 드라이브를 제어할 수 있도록 하며, 다음을 위한 훌륭한 도구가 될 수 있습니다.

- 개인 및/또는 집단 암호화 USB 사용 정책의 수립 및 시행.
- 조직 내외로 데이터 이동 시 더 정확히 추적할 수 있는 파일 작업 감사
- 중요한 데이터 전송을 위한 원격 콘텐츠 백업 제공
- USB 분실 또는 손상 시 원격으로 장치 비활성화
- 패스워드를 잊어버린 경우 원격으로 패스워드 재설정 수행

이러한 방식으로 검증된 드라이브를 올바르게 관리하면 민감한 데이터가 복사 및 공유될 위험을 최소화할 수 있습니다. 또한 현대의 하드웨어 암호화 USB 드라이브는 의도한 수신자가 아닌 다른 사람이 파일 및 메시지에 액세스하거나 읽지 못하도록 방지하는 데 도움이 되는 수많은 추가 보안 기능을 제공합니다.

> 하드웨어 암호화가 소프트웨어 암호화보다 낫다고 생각합니다. 하드웨어 암호화와 소프트웨어 암호화 방법의 차이점은 무차별 공격에 대한 취약성 면에서 중요합니다. 하드웨어 암호화 장치의 경우 그러한 공격에 쉽게 굴하지 않습니다.
>
> - Tomasz Surdyk

암호화: 하드웨어 기반과 소프트웨어 기반 비교

기업체에서는 비용 때문에 소프트웨어 기반 암호화를 고려할 수 있지만 이는 약간 근시안적인 태도일 수도 있습니다. 소프트웨어 기반 솔루션은 호스트 장치의 암호화 리소스를 다른 프로그램과 공유하기 때문에 컴퓨터만큼이나 안전하며, 유지관리하지 않으면 취약해지는 소프트웨어 업데이트가 필요한 경우가 많습니다. 소프트웨어 암호화 USB 드라이브는 패스워드를 추측하기 위한 무제한의 무차별 공격을 받을 수 있으며, 이러한 드라이브에는 짧은 기간 내에 수백만 개의 문자 조합을 테스트할 수 있는 소프트웨어 기반의 사전 공격에 저항할 수단이 없습니다.

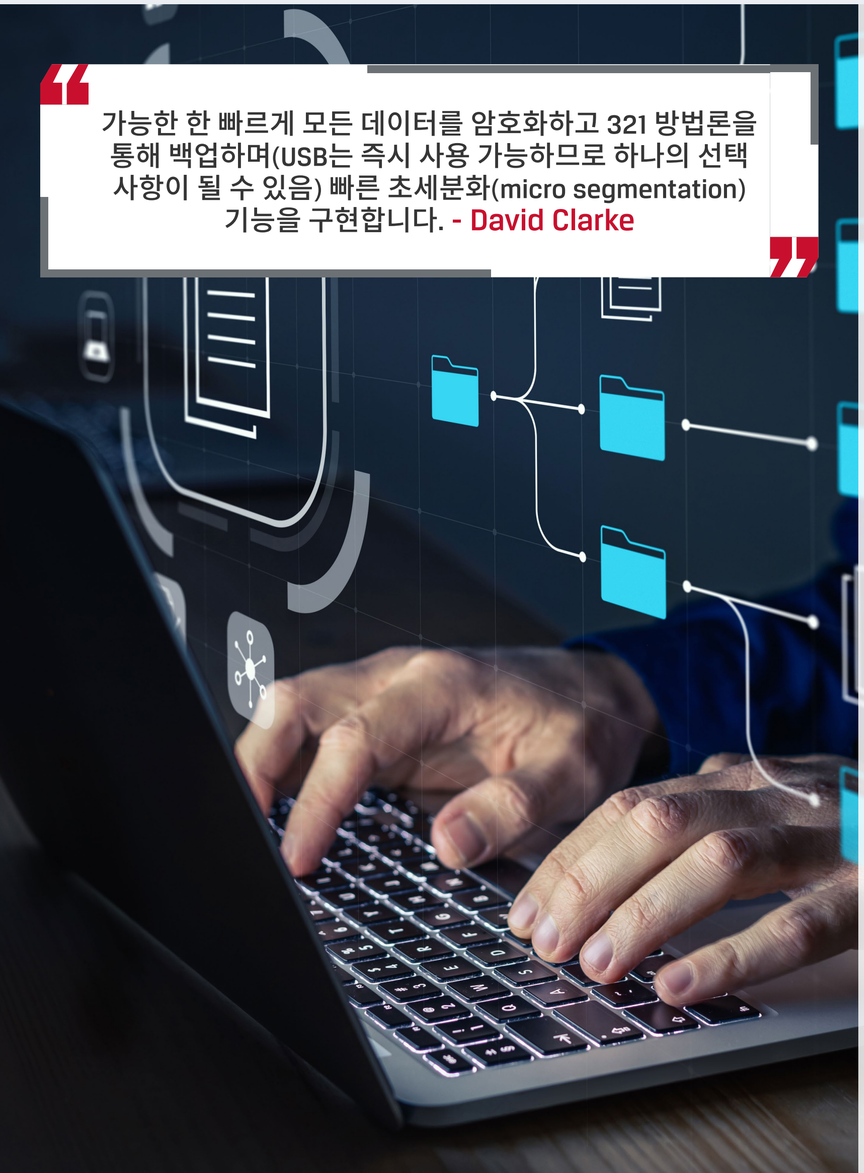
뿐만 아니라 소프트웨어 암호화 또한 이동식 암호화입니다. 소프트웨어 암호화 드라이브가 있는 직원이 데이터를 복사하고 USB 드라이브를 포맷하면 암호화가 제거됩니다. 그런 다음 데이터 파일을 다시 복사하면 다른 플랫폼 및 OS에서 인증하는 번거로움 없이 드라이브를 사용할 수 있습니다.

앞에서 언급했듯이 하드웨어 기반 암호화를 사용하면 물리적 “암호화” 및 이후 데이터 스토리지가 호스트 시스템과는 별개로 발생합니다. 그렇게 되면 시스템이 손상되더라도 추가 방어 계층이 보장됩니다.

이는 특히 금융, 의료 서비스, 정부 기관과 같은 업계 사람들로선 간과할 수 없는 부분입니다. HIPAA(Health Insurance Portability and Accountability Act, 건강보험이동성과 결과보고책무활동) 및 PCI DSS(Payment Card Industry Data Security Standard, 결제카드산업 데이터보안표준)와 같은 규정에는 민감한 정보의 암호화와 관련하여 엄격한 요건이 있는 경우가 많기 때문입니다.

강력한 하드웨어 암호화 장치를 사용하여 이러한 규정을 준수하면 결과적으로 조직에서 비싼 벌금, 소송 및 잠재적으로 심각한 평판 손상을 방지하는 데 도움이 됩니다. 하드웨어 암호화 드라이브는 더 저렴한 일반 USB 드라이브보다 비용이 많이 들 수는 있지만 침해에 대한 법적 비용은 고작 몇 시간 법률 상담료로 수백 개의 드라이브에 대해 쉽게 지불할 수 있습니다.

민감한 데이터를 보호해야 할 필요성 증가



> 가능한 한 빠르게 모든 데이터를 암호화하고 321 방법론을 통해 백업하며(USB는 즉시 사용 가능하므로 하나의 선택 사항이 될 수 있음) 빠른 초세분화(micro segmentation) 기능을 구현합니다. - David Clarke

민감한 데이터를 분실 및 도난 당하지 않게 보호하는 문제와 관련하여 모든 조직은 장치에 적절한 보안 기능이 있는지 확인할 의무가 있습니다. 또한 무수한 사이버 위협이 끊임없이 진화하는 가운데, 디지털 성숙도 수준과 사용자 본인의 엔드포인트 데이터 관리 기술이 해결되지 않을 경우 이는 두드러진 위험 요소로 남아 있다는 점을 고려하는 것도 중요합니다. 데이터 통제 또는 USB 저장 장치의 손실, 안전한 환경 외부로의 데이터 전송, 암호화되지 않은 USB 드라이브 사용, 패스워드 공유 등을 비롯한 내부 위협은 모두 최종 사용자 실사가 부족했던 결과일 수 있습니다. 적절한 훈련, 교육 및 올바른 USB 드라이브 솔루션을 사용하면 이 모든 문제를 방지할 수 있습니다.

사전 계획과 잘 실행된 커뮤니케이션 구조 또한 존재할지 모르는 위협을 처리하는 데 핵심 요소입니다. 오늘날의 사이버 위협은 조직의 약점을 공략하기 위한 것입니다.

귀하 조직의 전체 보안 전략에 암호화 USB 드라이브와 정책을 통합하여, 암호화 USB 계획이 실제로 필요해지기 전에 그 계획을 개발하는 것이 가장 좋습니다. 암호화 USB에 대한 계획을 갖추고 있지 않고 지침이 없다면, 아무것도 쌓아 나갈 수 없게 되며, 조직은 민감한 데이터를 암호화해야 한다고 구체적으로 명시하는 제32조의 GDPR(General Data Protection Regulation, 일반 데이터 보호 규정)과 같은 규정을 준수하지 않는 것을 포함하여, 모든 수준에서 위험에 노출됩니다.

> 조직은 데이터 연결을 물리적으로 제거하거나 해당 데이터 소스를 어둡게 하여 가장 중요한 데이터를 먼저 처리하는 계획과 함께 모든 데이터 세트의 중요성 및/또는 민감도 수준을 포함한, 데이터에 대한 명확한 청사진이 있어야 합니다. 영향받은 시스템을 신속하게 격리할 수 있느냐가 핵심입니다. 그리고 다시 말하지만, 실행에 옮긴 문서화된 계획을 갖추는 것이 절대적으로 중요합니다.
> - Rafael Bloom

> 사용자는 민감한 데이터를 처리합니다. 그러한 데이터를 손실할 경우 책임이 커지고 회사의 이미지와 안전에 큰 영향을 미칩니다. 민감한 데이터를 보호하려면 데이터 암호화를 비롯하여 다양한 보안 솔루션을 사용해야 합니다.
> - Tomasz Surdyk

민감한 금융 데이터 보호하기

보안 영향과 함께 데이터 스토리지 및 백업 솔루션이 준수해야 하는 규정 준수 기준들도 있습니다. 데이터 보존 일정을 관리 및 시행해야 할 필요성 등 이러한 관행 중 일부는 업종 전반에서 공통적인 반면, 기업용 데이터를 클라우드로 이동시키는 등과 같은 관행은 매우 다르게 취급합니다.

금융 서비스 등 많은 분야에서 적절한 데이터 관리를 의무화하는 규정이 시행되었습니다. 특히 은행의 경우 초반에 저장 및 백업을 위해 타사를 사용하기를 매우 꺼렸으며, 많은 은행에서 여전히 모든 데이터 인프라를 보유해야 한다고 주장합니다.

금융 기관은 또한 사베인스-옥슬리법(SOX, Sarbanes-Oxley Act) 및 GDPR(일반 데이터 보호 규정)과 같이 증가하는 데이터 보안 규정 및 기준 목록을 준수해야 합니다. 그러나 모바일 직원과 계약자의 수가 늘어나면서, 그에 따라 데이터 유출의 위험과 해당 법률 및 기준에서 부과한 의무사항을 준수하지 않을 위험 또한 증가합니다.

사실상, 모바일 직원이 디지털 ID, 휴대용 작업 공간, 고객 기록 및 지니고 있는 금융 데이터를 보호하지 못하면 규정을 준수하기 위한 노력은 놀라울 정도로 쉽게 손상될 수 있습니다. 따라서 점점 더 많은 조직이 Kingston IronKey 암호화 USB 드라이브와 같은 모바일 보안 솔루션 쪽을 택하여, 직원이 어디에 있든 상관없이 디지털 ID와 애플리케이션을 보호하고 있습니다.

> 더욱 분산적인 IT 공간으로 전반적인 추세가 변화하고 있다는 점과 클라우드 인프라의 순전한 확장성을 고려할 때 대부분의 산업과 상당수의 SME가 냉장 서버실 관리에 더 이상 관심을 두지 않는다는 사실을 쉽게 알 수 있습니다.
> - Rafael Bloom

환자 건강 데이터에 대한 보안 액세스

의료 서비스는 데이터 보안이 그 어느 때보다도 중요한 또 다른 산업 분야의 예입니다. 2021년에는 침해 건으로 4,567만 명의 환자 기록이 노출되어 2015년 이후 가장 많은 연간 총계를 기록하는 등 환자 정보가 도난당할 위험이 훨씬 더 커졌습니다[2]. 데이터 저장 및 백업과 관련하여 환자 데이터는 의료 제공자가 환자를 안전하게 치료할 수 있도록 하는 중요하고 포괄적인 의료 정보입니다.

이러한 의료 정보는 건강 기록, 검사, 사진 및 방사선 영상이 포함된 환자 전자건강기록(EHR, Electronic Health Record) 파일부터 급여 기록, 환자 보험 및 미지급금을 포함한 관리 파일에 이르기까지 모두 총망라할 수 있습니다. 점점 늘어나는 모바일 인력과 중대한 격변 및 전환을 겪고 있는 글로벌 의료 서비스 시장에 직면해 있는 오늘날의 의료 서비스 제공업체가 데이터 보안에 관심을 보이는 것도 놀라운 일은 아닙니다.

> 특히 랜섬웨어는 성장 산업의 일부이기 때문에 민감한 데이터를 취급하는 모든 조직은 극한의 압박 속에 운영하는 방법을 고려해야 합니다. - Rafael Bloom

또한 위험을 예측 못하고 HIPAA(건강보험이동성과 결과보고책무활동) 또는 HITECH(Health Information Technology for Economic and Clinical Health Act, 경제 및 임상 건강을 위한 건강 정보 기술법)와 같이 엄격한 필수 사항을 준수하지 않을 경우, 비용이 많이 드는 의료 서비스 데이터 침해가 발생할 수 있으며, 이는 환자, 파트너 또는 규제 기관의 신뢰를 한층 떨어뜨릴 수 있습니다.

Kingston IronKey 암호화 USB 드라이브와 같은 솔루션을 통해 의료 서비스 기관에서는 단일 콘솔에서 소수 또는 수천 개의 드라이브에 걸쳐 패스워드, 애플리케이션 사용, 복구 등에 대한 정책을 설정할 수 있습니다. 모바일 및 일선 작업자는 저장된 데이터에 안전하게 액세스하기 위해 사용자 친화적인 솔루션을 통해 직원이 드라이버 또는 기타 소프트웨어를 설치하지 않고도 더 많은 환자를 지원할 수 있습니다. 그리고 사용자 및 관리자는 데이터가 어디에 있든 손쉽고 빠르게 잠글 수 있습니다.

클라우드 스토리지의 미래에서 USB 드라이브의 위치

> 클라우드 데이터 스토리지는 현재이자 미래입니다. 저는 여전히 예컨대 암호화 USB 드라이브를 사용하여 물리적으로 데이터를 보호하는 것이 가장 안전하다고 주장합니다. 사용자는 클라우드에서 일어나는 일을 완전히 통제할 수 없습니다. 그러나 당사는 암호화 USB 드라이브의 데이터를 통제할 수 있으며, 이 드라이브를 자체적으로 보호하고 저장합니다. 우리 외에 아무도 이러한 미디어에 액세스할 권한이 없습니다. - Tomasz Surdyk

이제 USB 드라이브의 이점이 분명해졌습니다. 클라우드 스토리지의 미래에서 USB 드라이브의 역할은 정확히 무엇일까요?

10년 전에 USB 드라이브는 데이터를 편리하게 저장하고 전송하기 위한 기본 도구로서 엄청난 수요가 있었습니다. 그러나 새로운 하이브리드 작업 모델과 점점 더 분산되는 팀의 영향으로, 클라우드는 이제 많은 장치에서 저장된 정보로의 빠르면서 간단한 액세스가 가능하도록 해줍니다. 플래시 드라이브는 파일 전송에 있어 그 독특한 편안함으로 인해 한때 대단한 인기를 끌었습니다. 오늘날 클라우드 스토리지 서비스는 파일 이동성을 더욱 용이하게 합니다.

그러나 클라우드 스토리지에는 여전히 많은 한계점이 존재합니다. 파일을 백업하거나 전송할 수 있는 방법과 시기를 결정할 뿐만 아니라 그 밖의 보안 문제가 추가되는 네트워크 연결이 필요합니다. 회사에서 클라우드 사용을 의무화하는 경우, 그렇다고 해서 데이터 액세스 위치를 반드시 통제할 수 있는 것은 아닙니다. 따라서 개인 또는 공용 Wi-Fi 연결을 사용하여 VPN에 액세스하는 간단한 작업은 해킹당할 위험이 있습니다. 또한 클라우드 서비스는 모든 맬웨어의 다수(61%)가 현재 클라우드 애플리케이션을 통해 전달되므로 위협 행위자에게 매우 매력적인 대상입니다[3].

> 클라우드를 사용할 수 없는 경우 어떤 일이 발생하는지, 그리고 데이터가 100% 사용 가능해야만 하는 시나리오 및 장기간의 저장이 취약성을 야기할 수 있는 시나리오에 대해 고려하는 것이 현명할 수 있습니다. - David Clarke

클라우드 스토리지의 미래에서 USB 드라이브의 위치

반면에 USB 암호화는 장치의 하드웨어나 소프트웨어를 통해 이루어질 수 있습니다. 하드웨어 중심의 소프트웨어 없는 암호화는 사이버 공격으로부터 보호할 수 있는 가장 효과적인 방법입니다. 데이터 침해로부터 보호하는 탁월하면서 복잡하지 않은 솔루션으로, 데이터 보호의 궁극적인 보안을 통해 엄격한 규정 준수 기준을 충족하여 조직이 자신 있게 위협을 관리하고 위험을 줄이는 데 도움이 될 수 있습니다.

하드웨어 암호화 USB 드라이브는 독립적이기 때문에 호스트 컴퓨터에 소프트웨어 요소가 필요하지 않습니다. 소프트웨어 취약성이 없기 때문에 무차별, 스니핑 및 메모리 해시 공격이 발생할 가능성도 사라집니다. 소프트웨어 암호화 USB 드라이브는 또한 모든 사용자가 컴퓨터에서 드라이브를 포맷한 다음 그 드라이브를 사용하여 민감한 데이터를 무방비하게 저장함으로써 암호화를 비활성화할 수 있는 위험에 직면해 있습니다.

하드웨어 암호화 USB 드라이브는 또한 데이터 보안을 유지하는 탁월한 물리적 수단을 제공합니다. 이 드라이브는 사용자 또는 관리자가 정보 액세스 기준을 설정할 수 있도록 허용하며, 기존의 로컬 엔드포인트 솔루션과 통합할 수 있습니다. 그러므로 클라우드 스토리지가 작동하지 않거나 솔루션만큼 효과적이지 않은 많은 시나리오에 대해 편리하면서 비용 효율적인 솔루션이 됩니다. 네트워크에 연결되지 않은 장치에서 데이터를 저장해야 하는 경우, 비공개여야 하는 경우, 또는 오프라인일 때 액세스해야 하는 경우에 그럴 수 있습니다.

> 데이터가 조직에 평소에 활용되는 정도에 따라 '핫' 또는 '콜드'라고 간주한다면, 조직 또는 특정 비즈니스 핵심 기능 또는 프로세스에 있어 운영 지속성 및 고성능이 더 중요한 경우, '콜드' 데이터를 클라우드에 저장하고 '핫' 데이터는 로컬화된 USB 스토리지 쪽에 의존하는 것이 더 효율적일 수 있습니다. - Rafael Bloom

요약

미래 혁신의 도래를 예측할 수는 없지만 당사에서 제공할 수 있는 것은 수상 경력에 빛나는 USB 드라이브 포트폴리오로서, 이는 모든 수준의 모바일 데이터 보호 요건에 대한 동적 범위의 암호화 솔루션을 제시합니다. 사용하기 쉬운 PIN 보호를 위한 영숫자 키패드가 있는 USB 드라이브부터, 안티탬퍼링(anti-tampering) 보호 기능과 함께 최고 수준의 암호화를 위한 FIPS 140-2-Level 3 인증, 그리고 보안에 대해 타협하지 않는 SuperSpeed USB 3.1 기술에 이르기까지, Kingston IronKey 제품은 강력하고 효과적인 데이터 전송과 모바일 데이터 스토리지 솔루션을 약속하는 USB 드라이브를 통해 데이터 문제를 해결할 수 있도록 설계되었습니다.

당사의 특수 전문가 팀은 데이터 스토리지 여정의 모든 단계마다 귀하를 지원할 준비가 되어 있으며, 귀하의 요구사항을 충족하는 올바른 스토리지 솔루션을 찾을 수 있도록 신뢰할 수 있는 도움을 제공합니다.

암호화 USB 계획을 구축하려 하든, 비즈니스에 가장 적합한 USB 드라이브를 식별하고자 하든, 또는 보안 정책을 수립 및 시행하려는 경우이든 관계없이 귀하가 기밀 정보를 안전하게 유지하고 새로운 규정을 준수할 수 있도록 도와주는 기술과 기술적 능력을 갖추고 있습니다. 당사는 고도로 개인화된 서비스로, 귀하의 데이터 스토리지 우선 순위를 지원하는 제품을 제공하기 위해 최선을 다하고 있으며, 이를 통해 오늘날 전례 없는 속도로 변화하는 비즈니스 업계에 발맞추어 나아갈 수 있도록 해드립니다.

Kingston 소개

Kingston은 35년의 경험으로, 모바일 데이터 문제를 식별하고 해결할 지식을 보유하고 있으며, 그리하여 귀사 직원이 조직을 위태롭게 하지 않으면서 안전하게 업무를 할 수 있도록 도와드립니다.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou