Seagate Instant Secure Erase 사용 옵션

기술 백서

서론

폐기 처리될 하드 드라이브가 데이터 센터를 떠나 다른 사람 손에 들어가게 되는 경우, 이러한 드라이브에 저장된 데이터의 보안은 큰 위험에 노출됩니다. 그럼에도 불구하고 여전히 IT 부서는 다음과 같은 이유로 계속해서 드라이브를 퇴출 및 폐기해야 합니다.

- 다른 스토리지 목적을 위한 드라이브 용도 변경
- 보증, 수리 또는 대여 만료 등으로 인한 반환

드라이브가 데이터 센터에서 퇴출되는 경우 거의 모든 하드 드라이브가 원소유자의 통제를 벗어나게 됩니다. 실제로 Seagate는 데이터 센터에서 매일 50,000대의 드라이브가 퇴출되는 것으로 추정합니다. 이러한 드라이브에는 회사나 개인의 중요 자료가 담겨져 있으며 데이터 센터에서 퇴출되어도 데이터를 판독할 수 있습니다. RAID 데이터 보호로 구성된 스토리지 시스템의 여러 드라이브에 걸쳐 스트라이핑된 데이터조차도 보안에 취약합니다. 오늘날의 대용량 어레이에 포함된 스트라이프 하나만 해도 수백 명의 이름, 주민등록 번호 및 기타 개인의 중요한 데이터를 저장할 수 있을 만큼 크기 때문입니다.

드라이브 관리의 수고로움 및 폐기 시 비용

데이터 침해 및 이에 뒤따르는 데이터 보호 법률에 의한 고객에의 통지를 방지하기 위해, 기업은 퇴출 대상 드라이브가 관리 범위에서 벗어나 잘못된 손에 들어가기 전에 데이터를 완전히 삭제하기 위한 갖은 방법을 시도해 왔습니다. 현재는 이러한 방법의 일환으로 데이터를 판독 불가 상태로 변환시키고 있으나, 일반적으로 이 작업에는 인력이 상당히 많이 필요하고 이에 따른 기술적인 결함이나 인력으로 인한 실수가 발생할 수 있습니다.

오늘날 드라이브 처리 시 문제점은 종류도 다양할 뿐 아니라 그 범위 또한 광범위해졌습니다.

- 드라이브 데이터를 덮어 쓰는 경우 비용이 상당하며 주요 시스템 리소스를 몇 일간 사용하지 못할 수도 있습니다. 드라이브에서 덮어쓰기가 완료되었음을 알리는 메시지가 따로 생성되지 않을 뿐 아니라, 덮어쓰기를 통해 드라이브에서 재할당된 섹터를 커버하지 못해 데이터가 그대로 노출됩니다.

Seagate Instant Secure Erase 사용 옵션

- 드라이브를 디가우징(Degaussing)하거나 물리적으로 부수는 것 모두 상당한 비용이 요구됩니다. 디가우징 강도가 드라이브 유형에 최적화되어 있는지 알기는 어려울 뿐더러 드라이브에 판독 가능 데이터를 남겨둘 소지가 있습니다. 드라이브를 물리적으로 파손하는 것 또한 환경적으로 위험할 뿐 아니라 드라이브 보증 및 대여 만료를 위한 반환의 경우에는 불가합니다.
- 일부 기업에서는 드라이브를 안전하게 보안 유지하는 유일한 방법은 자신들의 관리 하에 두는 것이라고 생각하고 창고에 무한정 보관하는 방법을 택하기도 합니다. 하지만 이렇게 할 경우 점점 용량이 늘어나는 드라이브를 보관하고 관리하는 데 인력이 필요하게되면서 불가피하게 드라이브 도난 및 분실이 발생하고 결과적으로 전혀 안전하지 못한 방식이 됩니다. 실제로 Ponemon Group에서 수행한 2014년 데이터 침해 비용 연구에 의하면 데이터 침해 사고가 발생한 주된 요인은 악의적인 내부자 소행 또는 해커의 공격이었던 것으로 밝혀졌습니다.
- 일부 다른 기업에서는 전문 폐기 서비스 업체를 고용하여 서비스 관련 수행과 조정에 따른 비용과 내부 보고 및 감사에 드는 높은 비용을 추가로 들이기도 합니다. 그러나 이 경우 드라이브를 서비스 공급업체로 이송하면서 운송 중에 드라이브를 도난당하거나 분실할 가능성이 있어 또 다른 위험을 초래하게 됩니다. 드라이브 한 대만 분실해도 기업의 입장에서는 데이터 침해로 인한 손실이 수백만 달러가 될 수 있습니다.

이렇게 성능, 확장성 및 복잡성에 대한 요구가 점점 더 까다로워짐에 따라 IT 부서에서는 암호화를 사용해야 하는 보안 정책에서 퇴보하는 우를 범하게 되었습니다. 또한 암호화는 키 관리에 익숙하지 않은 기업에게는 자체 데이터는 언제든 해독할 수 있는 위험한 프로세스로 인식되기도 합니다. 자체 암호화 드라이브(SED)는 이러한 취약점을 포괄적으로 해결하여 드라이브 폐기 시 암호화가 더욱 빠르고, 쉽고, 편리해졌습니다.

Seagate의 Instant Secure Erase 기능을 통해 드라이브를 안전하면서도 신속하고 쉽게 폐기 및 용도 변경할 수 있습니다

SED는 드라이브 자체에 안전하게 저장된 데이터 암호 키를 이용하여 데이터가 드라이브에 들어올 때 모든 사용자 데이터를 암호화합니다. 따라서 SED에 저장된 모든 데이터는 기본적으로 암호화됩니다. 데이터 센터에서 드라이브를 퇴출하거나 용도 변경을 할 경우 드라이브에 명령을 전송하여 Seagate Instant Secure Erase(ISE)를 수행하기만 하면 됩니다. Seagate ISE는 SED의 암호화 영구 삭제 기능을 사용하여 데이터 암호 키를 변경합니다. Seagate ISE와 같은 암호화 키 삭제 방식은 현재 ISO(국제 표준화 기구) 및 NIST (미국립표준기술연구소)에서 권장하는 데이터 영구 삭제 방식입니다. 이는 "다른 영구 삭제 기법에 비해 훨씬 빠른 속도로 삭제를 확실하게 보장하기 때문"입니다.[1] 암호화 영구 삭제는 그림 1에 나온 것처럼 SED 내의 암호 키를 안전하게 바꿉니다.

그림 1. Seagate Instant Secure Erase 프로세스

데이터를 암호화하기 위해 최초에 사용된 키가 바뀌면 이 키와 함께 암호화된 모든 데이터는 판독이 불가능하며 절대 복구할 수 없습니다. 이런 방식으로 Seagate ISE는 기기에 저장된 데이터를 즉시, 안전하게, 효율적으로 파괴하므로 해당 드라이브는 곧장 폐기, 재사용 또는 판매할 수 있게 됩니다. 어떤 방식을 활용했는지에 상관없이 SED를 통해 IT 운영 비용이 줄어들기 때문에 드라이브 관리에 따른 문제점과 폐기 비용 문제를 한 번에 해결할 수 있습니다. Seagate의 정부 등급 데이터 보안 기능을 통해 IT 효율성을 저하시키지 않고도 데이터 개인 정보 보호 정책을 준수할 수 있습니다.

또한 SED는 다음과 같은 특성을 갖추어 처분 과정을 단순화하고 반환 및 용도 변경되는 하드웨어에 들어간 투자 비용을 보전할 수 있습니다.

- 드라이브를 덮어쓰거나 파손하여 폐기할 필요가 없음
- 보증 및 대여 만료 반환 보장
- 이전의 데이터가 노출되지 않도록 확실히 보증하여 드라이브를 용도 변경하거나 판매할 수 있도록 함

[1] ISO/IEC 27040 (Information technology—Security techniques—Storage security); NIST 800-88 (Guidelines for Media Sanitization)

Seagate Instant Secure Erase 사용 옵션

다양한 보안 니즈를 충족시키는 Seagate의 다양한 솔루션

- Seagate Secure 드라이브는 두 가지 종류로 출시되어 있습니다. 표준 SED 또는 FIPS(연방정부 정보처리 표준) 140-2 인증을 받은 모델을 선택하면 보안이 한층 강화됩니다. 두 종류 모두 Seagate Instant Secure Erase 기능을 탑재하고 있습니다. 따라서 고객은 단 몇 초 만에 드라이브 내용을 신속하고 안전하게 삭제할 수 있습니다.
  이 기능은 비암호화 드라이브에서는 이용할 수 없는, 매우 유용한 기능입니다.

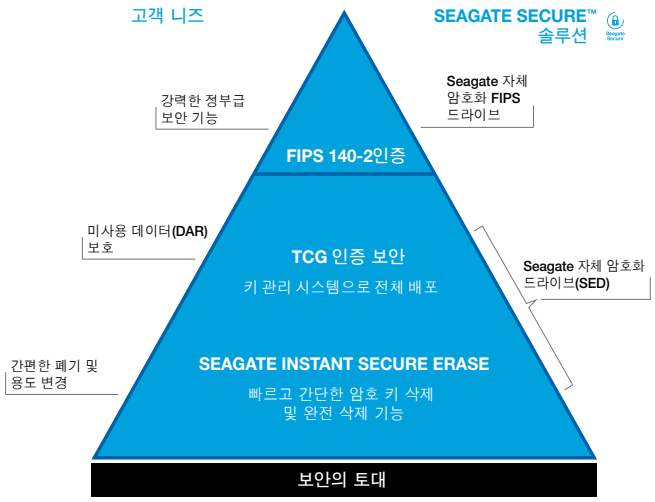

그림 2. 전 레벨의 보안 구현을 위한 Seagate Secure™ 솔루션

Seagate 자체 암호화 드라이브의 Instant Secure Erase 수행 방식

Seagate SED는 드라이브의 인터페이스 명령어 세트와 구성에 따라 Seagate ISE를 실행하는 여러 방법을 지원합니다. 가장 안전한 방법은 드라이브의 SED TCG(Trusted Computing Group) 보안 프로토콜을 통해 이용할 수 있는 암호화 영구 삭제 옵션을 이용하는 것입니다. 이 방식을 취하면 탁월한 보안 기능이 보장될 뿐만 아니라 신속하고 간편합니다. 고객은 기존의 데이터 덮어쓰기 명령 방식으로 드라이브를 삭제할 수도 있으나, 이 방법은 대체로 보안성이 떨어지는 것으로 간주되며 시간이 아주 오래 걸릴 수도 있습니다. 표 1에는 이를 포함한 여러 가지 데이터 삭제 방식이 제시되어 있습니다. 유념할 것은 어떤 경우에서도 호스트 컨트롤러는 지원되는 명령어를 통해 Seagate ISE를 지원하도록 구현해야 한다는 점입니다.

1. 미사용 데이터 보호 기능을 탑재하여 구성한 드라이브는 고급 FIPS 140-2 위변조 방지 기능 포함 여부와 무관하게 TCG 보안 프로토콜을 사용하여 활성화됩니다.

   TCG의 스토리지 규격 프로토콜을 사용하여 관리되는 SED는 대역 수준의 암호화 삭제(crypto erase)를 지원합니다. 대역 수준 암호화 삭제 방식은 드라이브를 사용하는 동안 사용자 데이터를 보호할 뿐만 아니라, 기기에 저장된 데이터의 일부나 전부를 삭제하면서도 해당 드라이브의 다른 데이터 대역에 영향을 미치지 않습니다. 이 전자 삭제 방식을 이용하려면 타사 소프트웨어가 필요합니다(Seagate의 여러 파트너사에서 제공).

   TCG 스토리지 규격 프로토콜을 통해 관리되는 SED를 완전히 삭제하는 또 다른 방법은 이 프로토콜의 RevertSP 명령어를 호출하는 것입니다. 이 유형의 보안 영구 삭제 방식을 이용하려면 라벨에 인쇄된 32자 길이의 PSID(물리적 보안 ID)를 읽기 위해 실제로 기기를 점유해야 합니다. 이렇게 해야 데이터를 안전하게 삭제하고 드라이브를 원래의 공장 상태로 구성할 수 있습니다.

2. 완전한 미사용 데이터 보호 기능을 사용하여 구성되지 않은 드라이브를 활성화하려면 ATA 보안 명령어를 사용하면 됩니다.

   ATA 명령어 세트를 구현하는 Seagate SED를 삭제하려면 ATA Security Erase Prepare 및 Security Erase Unit 명령어를 호출하면 됩니다. 이것이 Seagate ISE에 Seagate가 고유하게 구현한 방식입니다.

Seagate Instant Secure Erase 사용 옵션

표 1은 SED에서 데이터를 삭제하는 여러 가지 방법을 간략히 보여줍니다. 표 아래 나오는 메모를 참조하십시오.

표 1. Seagate Instant Secure Erase 옵션

초기 구성	미사용 데이터 보호(위변조 증거 보호 포함 또는 미포함)		제한된 보안 적용됨	보안 적용하지 않음
영구 삭제 방식	**TCG 보안 프로토콜** 영구 삭제	**TCG 보안 프로토콜** RevertSP	**ATA 보안** Security Erase Prepare 및 Security Erase Unit 명령어	**완전 삭제** 완전 삭제 기능 세트/명령어
지원되는 구성	TCG 인증 Seagate SED 스토리지	TCG 인증 Seagate SED 스토리지	Seagate SATA SED	지원되는 Seagate SATA 및 SAS SED
영구 삭제 범위	대역 수준 암호화 영구 삭제	암호화 방식으로 전체 드라이브 영구 삭제	암호화 방식으로 전체 드라이브 영구 삭제	암호화 방식으로 전체 드라이브 영구 삭제
부작용	밴드 잠금 해제 및 밴드 비밀번호 리셋	SED가 공장 기본 상태로 돌아감	드라이브 잠금 해제 및 ATA 보안 비활성화	우발적 영구 삭제를 방지할 초기 보안 없음
액세스 제어	호스트-관리 또는 기기의 기본 비밀번호를 통한 인증이 필요	드라이브 라벨에 인쇄된 (및 바코드 형식의) 비밀번호를 통한 인증 필요	호스트-관리 비밀번호를 통한 인증이 필요	기본적으로 인증 없음(드라이브가 잠긴 경우, 실행 전에 조작자가 드라이브의 잠금을 해제해야 함)
장점	미사용 데이터(DAR) 보호 FIPS 140-2 레벨 2 인증 TCG 스토리지 사양을 기반으로 한 다양한 기능의 보안 관리 인터페이스	미사용 데이터(DAR) 보호 FIPS 140-2 레벨 2 인증 TCG 스토리지 사양을 기반으로 한 다양한 기능의 보안 관리 인터페이스	드라이브 수준 보안 보안이 표준 ATA 보안 명령어를 사용함	관리 비용 없이 보안 영구 삭제 기능 제공(즉, 비밀번호 관리 불필요)
비고	TCG 호환 하드웨어 또는 소프트웨어 필요	드라이브 보안 코드를 판독하기 위해 물리적으로 SED의 공간 점유 필요	표준 ATA 보안 명령어 활용	명령어의 비보호적인 특성상, 실수나 악의적인 데이터 영구 삭제 가능성

참고

1. 대부분의 경우, 높은 보안 구성으로 드라이브를 안전하게 영구 삭제하는 방법은 낮은 보안 설정에 이용될 때도 효과가 있습니다. 예를 들어, RevertSP 방식은 ATA 모드로 구성된 드라이브에도 효과가 있는데, 그 이유는 이 드라이브가 TCG 명령어 세트도 지원한다고 가정하기 때문입니다(보안 지원은 드라이브 모델마다 다를 수 있습니다).
2. *미사용 데이터(data-at-rest) 보호*라는 말은 작동하는 컴퓨터 환경에 있는 동안 무단 액세스가 있을 때 데이터 인터페이스를 잠그도록 구성된 드라이브의 데이터를 유출로부터 매우 강력히 보호하는 SED의 기능을 가리킵니다.
3. FIPS(연방정부 정보처리 표준) 간행물 140-2는 암호화 모듈을 인증하는 데 사용되는 미국 정부 컴퓨터 보안 표준입니다. 간행물의 제목은 *Security Requirements for Cryptographic Modules(FIPS PUB 140-2)*이며 NIST(국립표준기술연구소)에서 발간합니다. 이 표준에서 명시하는 보안 요건을 충족하려면 *중요하지만 기밀은 아닌 보호* 등급 데이터를 보호하는 보안 시스템 내에서 활용하는 암호화 모듈이 필요합니다. Seagate FIPS 드라이브는 보안 레벨 2(위변조 증거) 인증을 받았습니다. 보다 자세한 내용은 다음 문서를 참조하십시오: http://www.seagate.com/files/www-content/solutions-content/security-and-encryption/en-us/docs/faq-fips-sed-mb605-3-1411us.pdf

Seagate Instant Secure Erase 사용 옵션

Seagate SED에서 Seagate Instant Secure Erase를 수행하는 방법

장치를 안전하게 영구 삭제하기 위해 선택한 옵션과 SED의 종류에 따라 여러 방법으로 데이터를 실제로 영구 삭제할 수 있습니다. 다음과 같은 솔루션을 이용할 수 있습니다.

- Windows용 Seagate SeaTools™ 소프트웨어: 내장형 및 외장형 연결 방식 스토리지 기기를 모두 진단하는 PC용 무료 툴입니다. SeaTools 소프트웨어는 Seagate ISE를 지원합니다. SeaTools 소프트웨어는 당사 웹사이트(www.seagate.com)에 방문하여 Support and Download(지원 및 다운로드) 탭의 SeaTools – Diagnosis Software(진단 소프트웨어)에서 다운로드할 수 있습니다.
- Seagate 파트너사에서 제작한 타사 키 관리 소프트웨어 애플리케이션(예: IBM(Tivoli Key Lifecycle Manager), Wave, WinMagic 등).
- 맞춤형/임베디드 솔루션은 Seagate ISE 기능을 시스템이나 호스트 애플리케이션에 통합합니다. 자세한 내용은 Seagate 영업 담당자에게 문의하십시오.
- Linux 사용자의 경우, 자신만의 SATA 명령어를 사용하고자 한다면 HDPARM(Linux 운영 체제용 명령줄 유틸리티)을 사용하면 됩니다.

참조 자료

TCG 스토리지 사양—
www.trustedcomputinggroup.org/developers/storage/specifications

ATA 사양—
www.t13.org/

SCSI 사양—
www.t10.org/

Seagate SeaTools 소프트웨어—
www.seagate.com/www/en-us/support/downloads/seatools/

Seagate Secure®

seagate.com

미주 Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, +1 408 658 1000
아시아/태평양 Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485 3888
유럽, 중동, 아프리카 Seagate Technology SAS 16-18 rue du Dôme, 92100 Boulogne-Billancourt, France, +33 1 41 86 10 00