FULL DISK ENCRYPTION

솔루션 개요

ESET Full Disk Encryption(EFDE)은 ESET 원격 관리 콘솔(ESET Cloud Administrator 및 ESET Security Management Center)의 기본 추가 기능입니다. 주요 기능은 사전 부팅 로그인 단계에서 추가 보안 계층을 사용하여 관리되는 Windows 워크스테이션의 전체 디스크 암호화 관리입니다.

시장 상황

사이버 보안의 일반적인 변화는 맬웨어로부터 엔드포인트를 보호할 뿐만 아니라 장치에 저장된 데이터를 보호하는 것입니다. 암호화는 SMB 고객의 데이터 보호 규정을 준수하는 데 필요한 기술적 조치 중 하나입니다.

고객 가치 제안

간단한 ESET 기본 전체 디스크 암호화 솔루션으로 회사 데이터 안전과 규정 준수를 보장합니다.

주요 판매 포인트

- 회사 컴퓨터의 보안 데이터.
- 데이터 규정 준수.
- 원격으로 암호화 관리 및 모니터링 기능.

대상 고객

엔드포인트에 저장된 조직의 데이터를 보호 하고 원격 관리 콘솔에 통합되는 솔루션이 필요한 고객

주요 특징들

잘 알려진 개념

ESET Full Disk Encryption 정책, 클라이언트 작업, 그룹을 통해 Endpoint 보안 제품과 동일한 개념을 기반으로 관리할 수 있습니다.

설치의 용이성

전체 디스크 암호화 섹션은 ESMC(ECA의 라이브 설치 프로그램)에서 생성할 수 있는 일체형 설치 프로그램에 추가됩니다. 설치 프로그램을 생성할 때 관리자는 EFDE의 라이선스와 사용 가능한 버전을 선택합니다. 또한 관리자의 전체 디스크 암호화 기본 설정에 따라 정책을 선택할 수 있습니다.

암호화 옵션

관리자에게는 소프트웨어 또는 하드웨어(OPAL 2.0 사용)의 두 가지 암호화 유형이 제공됩니다. 두 경우 모두 TPM(2.0 이상) 보안 칩을 선택하여 디스크 암호화 키를 추가로 보호할 수 있습니다.

비밀번호 정책

전체 디스크 암호화 솔루션의 주요 기능은 사용자의 저장 데이터를 보호하는 것입니다. 비밀번호의 강도 및 기타 속성이 중요한 역할을 합니다. 관리자는 필수 비밀번호 속성, 비밀번호 재시도 횟수 및 만료 기간을 설정하는 최종 권한이 있습니다. 정책 설정에서 사용자가 원할 때마다 암호를 변경할 수 있는 옵션을 부여할 수 있습니다.

즉시 조치를 위한 클라이언트 작업

관리자가 즉각적인 조치가 필요한 다양한 시나리오에서 신속하게 조치를 취할 수 있도록 전체 디스크 암호화 관련 작업이 표시됩니다. 디스크 암호화와 관련된 다소 심각한 상황에서 세 가지 작업을 사용할 수 있습니다.

1. "FDE 로그인 암호 차단"을 트리거하면 엔드포인트에서 사전 부팅 로그인이 비활성화됩니다. 시스템은 암호 복구만 사용하고 액세스를 복원하고 새 암호를 설정하여 부팅할 수 있습니다.

2. "FDE 로그인 암호 무효화" 작업은 사용자에게 클라이언트 EFDE 응용 프로그램에서 암호를 변경하도록 요청합니다.

3. "FDE 로그인 암호 지우기" 작업은 로컬 사용자 복구 정보를 포함하여 워크스테이션에서 암호화 키를 제거합니다. 시스템을 부팅할 수 없으며 암호화 복구 유틸리티에서만 복구가 가능합니다.

즉시 복구

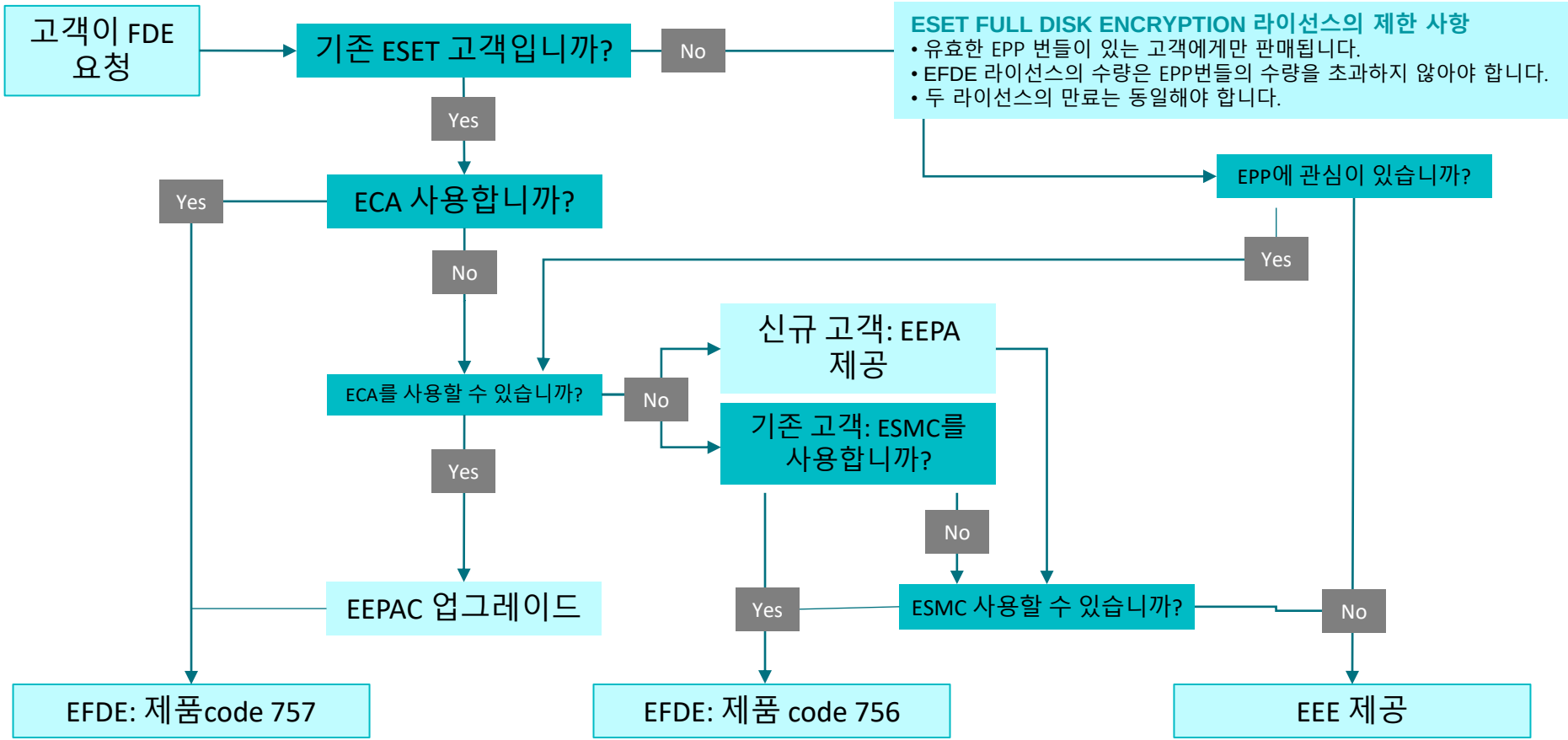
비밀번호 정책에 따라 사용자가 너무 많은 잘못된 비밀번호 시도로 인해 잠긴 경우 또는 분실 및 도난 된 시스템이 사용자에게 반환된 경우 관리자는 다음 중 하나를 적용하여 암호화된 시스템에 대한 사용자 액세스를 복원할 수 있습니다.

- "암호 복구" 방법은 빠르고 간단하며 사용자가 잠긴 후 액세스를 허용하는 가장 일반적인 방법입니다.
- "데이터 복구" 방법은 하드웨어 오류 또는 손상의 경우 "FDE 로그인 암호 지우기" 작업을 사용하여 시스템이 비활성화된 보다 심각한 경우를 위해 설계된 복구 유틸리티와 함께 사용할 복구 데이터를 생성합니다.

Endpoint에 있는 별도의 사용자 인터페이스

ESET Full Disk Encryptiont에서는 주로 시스템 암호화 상태를 표시하는 자체 애플리케이션 및 사용자 인터페이스가 있습니다. "설정" 섹션에서 사용자는 디스크 및 파티션의 암호화 상태를 볼 수 있으며 필요할 때마다 사전 부팅 암호를 변경할 수 있습니다. "도움말 및 지원" 섹션은 KB 문서, 기술 지원 및 온라인 도움말로 연결됩니다.

ESET 암호화 솔루션 제공 방법



ESET Full Disk Encryption

다른 ESET 보안 제품과 함께 클라우드 기반 또는 온프레미스 콘솔에서 전체 네트워크의 전체 디스크 암호화를 관리합니다. ESET Cloud Administrator 및 ESET Security Management Center를 사용하면 관리자가 클릭 한 번으로 연결된 끝점에서 암호화를 배포, 활성화 및 관리할 수 있습니다. 전체 디스크 암호화(FDE)는 시스템 디스크, 파티션 및 전체 드라이브를 암호화하여 각 PC 또는 랩톱에 저장된 모든 항목을 잠그고 안전하게 보호하여 분실 또는 도난으로부터 사용자를 보호합니다.

이럴 때 사용하세요

모든 제품은 하나의 콘솔에서 관리합니다.
IT 관리자는 매일 원격 관리를 처리합니다. ESET Full Disk Encryption는 ESET Cloud Administrator 또는 ESET Security Management Center 내에서 작동하므로 관리자가 기존 관리 환경 및 개념에 익숙해져 시간을 절약할 수 있습니다.

법규 준수를 위한 필수 암호화 솔루션입니다.
ESET Full Disk Encryption는 데이터 손실로부터 회사를 보호할 뿐만 아니라 GDPR과 같은 데이터 보호 규정을 준수하는 데도 도움이 됩니다. 이 솔루션은 각 최종 사용자의 장치에 저장된 데이터를 원격으로 암호화하는 간단하고 간단한 방법을 제공합니다.

vs

ESET Endpoint Encryption

추가 보호를 제공합니다. 사용자는 파일, 폴더, 이동식 미디어 및 이메일과 같은 개별 항목을 보호할 수 있습니다. 파일 및 이메일 암호화를 통해 데이터가 전송될 때 사용자 데이터가 보호되어 안전한 협업이 가능합니다. 또한 프록시를 통해 원격 장치를 관리할 수 있으므로 위험한 수신 연결이 필요하지 않으며 모든 규모의 기업에서 암호화를 안전하고 간단하게 관리할 수 있습니다.

이럴 때 사용하세요

세분화된 데이터 보호
모든 회사에는 고객 목록, 독점 정보 및 판매 관련 데이터와 같은 민감한 데이터가 있습니다. ESET Endpoint Encryption은 기업이 특정 **파일, 폴더, 가상 디스크 또는 아카이브**를 보호하는 향상된 기능을 제공합니다. 공유 장치 정책 및 고급 암호화 요구 사항이 있는 조직에 이상적입니다.

전송중인 데이터 보호
ESET Endpoint Encryption을 사용하면 회사 컴퓨터에 저장된 데이터만 보호되는 것이 아닙니다. 이메일 및 첨부 파일을 암호화하여
특정 사용자의 이동식 미디어에 대한 액세스를 제한하여 전송 중인 데이터를 보호하고 회사 외부로 유출되는 것을 방지할 수 있습니다.

특징	ESET Full Disk Encryption	ESET Endpoint Encryption
전체 디스크 암호화	•	•
이동식 미디어 암호화	•	•
파일 및 폴더 암호화	•	•
이메일 및 첨부파일용 Outlook 플러그인	•	•
가상 디스크 & 암호화된 아카이브	•	•
라이선스	기기 별/단일 사용자	사용자 별/다중 사용자
구매 옵션	ESET Endpoint solutions에 추가 기능	독립형 구독
MSP 월간 라이선스를 통해 사용 가능	•	•

추가 리소스

https://www.eset.com/int/business/full-disk-encryption

리셀러를 위한 EFDE 제품 게시판: GPC | Global Hub

ESET Encryption Solutions (EFDE vs. EEE제품 비교): GPC | Global Hub

ESET Online Help: https://help.eset.com/preview/efde/en-US/index.html

FAQ

DESlock 과는 다른 암호화 솔루션입니까??
ESET Endpoint Encryption(DESlock+)과 동일한 팀에서 생산하지만 제품은 다른 아키텍처와 다른 목적을 위해 구축되었습니다.

추가 클라이언트가 있습니까? 기존 에이전트와 신규 에이전트는 어떤식으로 구성되나요?
ESET Full Disk Encryption위한 추가 신규 클라이언트(응용 프로그램)이지만 ESMC와 통신하는 에이전트는 EM 에이전트와 동일합니다.

암호화 에이전트를 ESET Endpoint와 결합할 계획이 있습니까?
아니요, 계획에 없습니다.

ESET Endpoint Encryption은 Windows 시스템에만 적합합니까?
네.

ESET Full Disk Encryption에 사용되는 암호화 알고리즘은 무엇입니까? 구성이 가능한가요?
암호화는 256비트 AES를 실행하는 FIPS 140-2 인증 Windows Crypto API 또는 OPAL 2.0 호환 드라이브의 하드웨어와 함께 ESMC 디스크 암호화 드라이버에 의해 처리됩니다.

ESET Endpoint Encryption에서와 동일한 방식으로 ESET Full Disk Encryption에 SSO 정책을 적용할 수 있습니까?
아니요, '사용자 별' 및 '다중 사용자'인 EEE와 달리 EFDE는 '기기 별' 및 '단일 사용자'이므로 SSO가 없습니다.

EFDE/EPP 라이선스가 만료되면 암호화는 어떻게 됩니까?
라이선스 만료 후 14일이 지나면 사전 부팅 로그인 화면이 제거됩니다(컴퓨터는 0 키로 암호화된 상태로 유지). 이는 사용자가 Windows 로그인 자격 증명을 통해 시스템에 로그인할 수 있음을 의미합니다.

ESET Endpoint Encryption 평가판에서 정식 버전으로 변환하려면 디스크 암호를 해독한 다음 다시 암호화해야 합니까?
아니요, 문제 없이 갱신 됩니다. 위와 같은 문제가 발생된다면 라이선스가 만료되고 제품이 다른 라이선스로 재활성화 되는 경우입니다.

EFDE에서 EFDE Cloud로 마이그레이션할 때 라이선스 키가 변경됩니까?
EFDE 라이선스가 EFDE Cloud 라이선스로 업그레이드 또는 다운그레이드 된 경우 라이선스 키는 동일하게 유지될 수 있습니다.

다른 AV 공급업체를 사용하는 고객을 위해 엔드포인트가 없는 ESET Full Disk Encryption를 판매할 계획이 있습니까?
아니요. ESET Full Disk Encryption는 현재 고객 또는 EPP 라이선스를 구매하는 신규 고객에게 판매됩니다. 일반적으로 예외가 발생할 가능성은 항상 있지만 온프레미스 ESMC와 함께 사용하는 경우에만 가능합니다. ECA에서는 이것이 불가능합니다.

MSP의 경우 번들링이 사용되고 있는지 어떻게 확인할 수 있습니까?
MSP의 경우 번들링이 필요하지 않습니다.

암호화가 포함된 다른 제품인 Safetica와 FDE와 어떻게 경쟁합니까?
Safetica는 기술 제휴 제품이며 ESET Endpoint Encryption은 ESET의 핵심 제품입니다. 다른 기능의 경우와 같이 기능적 중복이 있을 수 있지만 이는 ECA를 비롯한 기본 관리 콘솔에 통합된 핵심 제품입니다.