cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryption Ransomware Protection

당면 과제: 비즈니스 중요 데이터에 대한 액세스를 차단하는 랜섬웨어

2020년 이후로 증가세를 보여온 랜섬웨어는 현재 전체 데이터 유출의 25%를 차지하고 있습니다.[1] 랜섬웨어 공격은 몸값을 지불할 때까지 중요 데이터에 대한 액세스를 차단하여 비즈니스 운영을 마비시킬 수 있습니다. 2031년이면 랜섬웨어가 2초마다 기업과 개인을 공격할 것으로 예상됩니다.[2]

차세대 방화벽이나 보안 이메일/웹 게이트웨이와 같은 경계 관리 도구를 사용하고 취약성 격차를 줄이는 데만 중점을 두는 기본적인 보안 전략으로는 랜섬웨어 공격을 막기에 역부족입니다. 포춘지 선정 500대 기업들은 엔드포인트와 서버에서 승인되지 않은 프로세스와 사용자가 비즈니스 중요 데이터를 암호화하지 못하도록 보호해야 하는 중요한 과제에 직면해있습니다.

솔루션: CipherTrust Transparent Encryption Ransomware Protection

CTE-RWP는 비간섭적인 방법으로 랜섬웨어 공격으로부터 파일/폴더를 보호합니다. 즉, 프로세스별로 비즈니스 중요 데이터를 호스팅하는 파일에서 비정상적인 I/O 활동을 감시합니다. 따라서 관리자는 랜섬웨어가 엔드포인트/서버를 장악하기 전에 의심스러운 활동에 대해 경보를 발행하여 공격을 차단할 수 있습니다.

주요 장점

- **투명한 데이터 보호.** CTE-RWP는 엔드포인트/서버의 어떤 애플리케이션도 수정할 필요 없이 최소한의 구성으로 볼륨별 랜섬웨어 보호 기능을 지속적으로 적용합니다. 또한, 랜섬웨어에 감염된 프로세스로 인해 발생하는 비정상적인 파일 활동을 지속적으로 모니터링하고 이러한 활동이 감지되면 경보를 발행해 공격을 차단합니다.
- **간편한 배포.** CTE-RWP는 관리자가 CTE 라이선스에서 사용할 수 있는 파일/폴더별로 제한적인 액세스 제어 및 암호화 정책을 설정할 필요 없이 랜섬웨어 보호 기능을 단독으로 적용할 수 있게 해줍니다.
- **강력한 랜섬웨어 탐지 기능.** CTE-RWP는 프로세스 기반의 머신 러닝 모델을 사용해 의심스러운 파일 I/O 활동을 동적으로 탐지합니다. 또한, 엔드포인트/서버에서 랜섬웨어를 식별해서 경보를 발행하거나 공격을 차단합니다. 승인된 프로세스를 신뢰할 수 있는 목록에 추가하면 모니터링을 우회할 수 있습니다.

1 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
2 https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/#:~:text=Cybersecurity%20Ventures%20predicts%20that%20by,than%20ever%20protecting%20against%20ransomware

라이선싱

CTE-RWP는 라이선스가 별도로 부여됩니다. 각 엔드포인트/서버의 파일/폴더 수준에서 상세한 액세스 제어 정책을 마련하지 않고도 적정 수준의 랜섬웨어 탐지가 가능합니다. 관리자는 CTE 라이선스를 함께 사용하여 보다 세분화된 액세스 제어와 암호화를 추가로 적용할 수 있습니다. CTE-RWP는 별도로 라이선스를 구매하거나, CTE 라이선스를 함께 사용할 수 있습니다.

CipherTrust Transparent Encryption을 통해 랜섬웨어로부터 데이터 보호를 강화

고객은 CTE(CipherTrust Transparent Encryption)용 라이선스를 추가하여 엔드포인트/서버에서 랜섬웨어를 최대한 보호함으로써 다음과 같이 CTE-RWP에서는 제공하지 않는 추가적인 이점을 얻을 수 있습니다.

세분화된 액세스 제어

- 비즈니스 중요 데이터가 상주하는 디렉토리에 대한 암호화/복호화/읽기/쓰기/목록 작성 권한을 가진 사용자/그룹을 정의
- 데이터 유출을 방지하기 위한 백업 암호화를 포함해 백업 프로세스에 엄격한 액세스 제어 정책을 적용
- 무결성을 보장하기 위해 신뢰할 수 있는 애플리케이션에 대한 서명 확인을 포함하는 보호된 폴더에 액세스하고 암호화/복호화하도록 승인된 가드 포인트 수준으로 신뢰할 수 있는 파일(바이너리) 목록

저장 데이터 암호화

- 온프레미스에 상주하든 클라우드 상주하든 관계없이 비즈니스 중요 데이터를 암호화
- 데이터가 암호화되어 있기 때문에 침입자가 금전 갈취를 위해 중요 데이터를 게시하겠다는 협박을 할 수 없음
- 무결성을 보장하기 위해 신뢰할 수 있는 애플리케이션에 대한 서명 확인을 포함하는 보호된 폴더에 액세스하고 암호화/복호화하도록 승인된 가드 포인트 수준으로 신뢰할 수 있는 파일(바이너리) 목록

CipherTrust Encryption용 MFA 사용

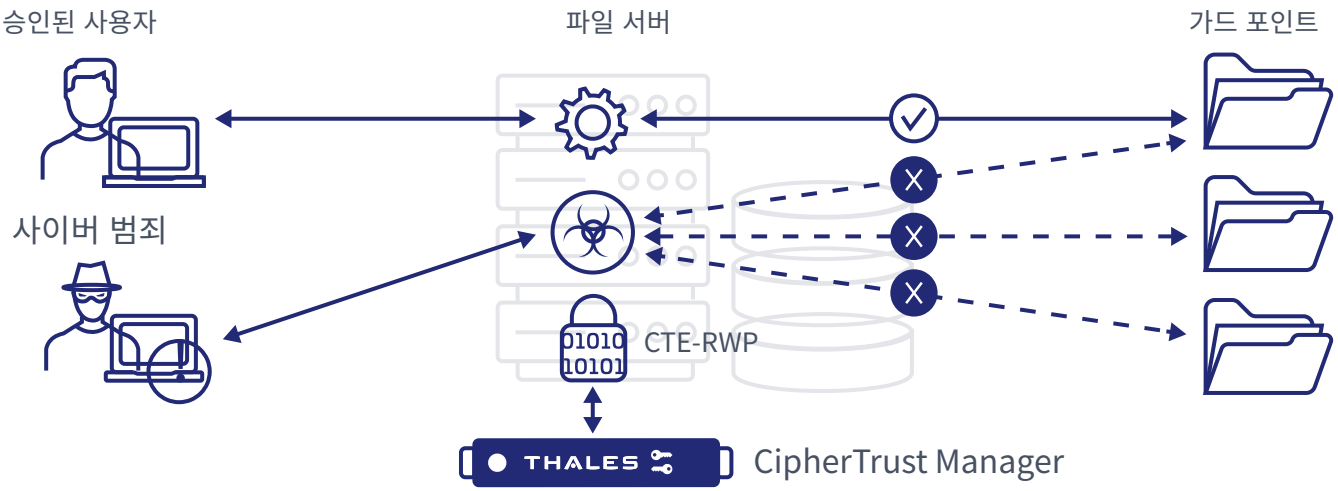
고객은 CTE(CipherTrust Encryption)용 MFA(Multi-Factor Authentication)를 추가하여 폴더/파일 수준에서 별도의 보호 계층을 구축할 수 있습니다. CTE용 MFA는 시스템 관리자와 권한 있는 사용자가 가드 포인트 뒤에 상주하는 중요 데이터에 액세스를 시도할 때 비밀번호 이외에 별도의 인증 요소를 제시하도록 요청합니다.

CTE용 MFA는 Windows 플랫폼에서 사용할 수 있습니다. 또한, 탈레스의 SafeNet Trusted Access, Okta, Keycloak 등 여러 인증 공급업체의 제품과도 통합됩니다.

탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련하여 갈수록 결정적인 순간을 맞이하고 있습니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 디지털 트랜스포메이션을 지속할 수 있습니다.

결단이 필요한 순간을 위한 결정적인 솔루션



CTE-RWP(CipherTrust Transparent Encryption - Ransomware Protection)