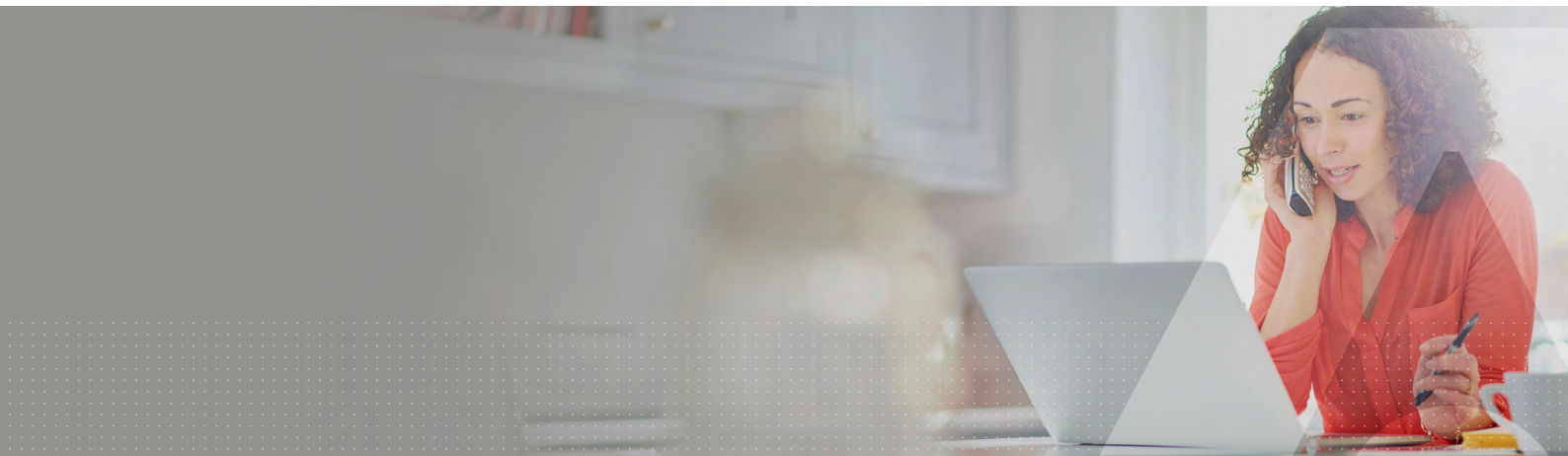


# 구글 워크스페이스용 탈레스 보안 솔루션

## 구글 워크스페이스 클라이언트 측 암호화와 탈레스 아이덴티티 및 데이터 보안 통해 향상된 개인 정보 보호와 기밀성



### 구글 워크스페이스를 위한 향상된 키 관리

디지털 혁신과 클라우드 기반 애플리케이션의 세계에서 클라우드 공급자와 기업은 보다 강력한 클라우드 보안 및 규정 준수를 모색하고 있습니다. 이러한 과제를 해결하기 위해 구글 워크스페이스는 클라이언트 측 암호화 솔루션(베타출시 예정)을 통해 향상된 개인 정보 보호 및 기밀 옵션을 제공합니다. 이 솔루션은 SafeNet Trusted Access와 CipherTrust Cloud Key Manager를 함께 사용하여 기업고객이 암호화 키를 완전히 제어할 수 있는 솔루션입니다.

'공유 보안'의 개념을 준수하는 구글은 EKM(external key manager, 외부 키 관리)과 IDP(Identity Provider, 아이덴티티 제공자)를 사용하여 오직 권한이 있는 인증된 자만이 보호되는 문서에 액세스할 수 있도록 조치할 것을 권장하고 있습니다. 오직 탈레스만이 독립적인 IDP와 키 관리 솔루션을 개발하고 있습니다.

### 탈레스 아이덴티티 보호 및 키 관리 기능을 갖춘 구글 워크스페이스 클라이언트 측 암호화 : 결합을 통한 성능 향상

구글 워크스페이스 클라이언트 측 암호화를 사용하는 고객은 아이덴티티를 보호하고 클라우드 내 중요 데이터와 별개로 암호 키를 제어하는 탈레스의 통합된 엔드 투 엔드 솔루션을 이용하여 보안을 한층 강화하면서 배포 비용을 절감할 수 있습니다.

클라이언트 측 암호화 키를 사용하면 서비스 공급자가 암호화된 데이터를 호스팅할 수는 있지만 해독할 수 없으므로 사용자의 개인 정보가 보호됩니다. 사용자가 자신의 파일을 검색하는 경우에 고객 제어 인증을 통해 사용자 인증을 거쳐야 합니다. 그런 절차를 거쳐야만, 고객이 제공한 키를 사용해 해당 데이터 암호 키의 암호를 해독할 수 있습니다.

CipherTrust Cloud Key Manager와 함께 사용되는 탈레스의 STA(SafeNet Trusted Access)는 고객에게 단일 벤더의 독립적인 IDP와 키 관리 솔루션을 제공하여 고객이 원활한 배포와 우수한 사용자 경험 및 더 나은 가치를 통해 비즈니스 목표를 달성할 수 있도록 지원합니다.

탈레스는 믿을 수 있는 멀티 클라우드 파트너입니다. STA와 CipherTrust Cloud Key Manager가 결합되어 조직이 벤더 종속성을 피하면서 액세스 보안과 키 관리를 함께 제어할 수 있습니다. 이는 디지털 전환 계획의 일환으로 멀티 클라우드 환경을 지원하는 데 필수적입니다.

## 공동 솔루션의 작동 원리

사용자가 구글 워크스페이스에 로그인하면 인증과 아이디 검증을 위해 STA로 리디렉션됩니다.

- STA가 사용자를 인증하고 인증 토큰을 생성합니다.
- 사용자가 클라이언트 측 암호화된 파일을 생성하면 STA에서 생성한 인증 토큰과 구글에서 생성한 별도의 인증 토큰이 구글에서 생성한 DEK(Data Encryption Key, 데이터 암호화 키)와 함께 CipherTrust Cloud Key Manager로 전송됩니다.
- CipherTrust Cloud Key Manager는 STA에서 생성한 인증 토큰을 STA로 검증하고, 구글에서 생성한 인증 토큰을 구글로 검증합니다.
- 두 토큰의 검증이 완료되면 CipherTrust Cloud Key Manager가 CipherTrust에서 생성한 KEK(Key Encrypting Key, 키 암호화 키)로 DEK를 암호화하여 이를 구글로 반환합니다.
- 이후 파일을 열람하거나 저장하려면 권한 있는 당사자가 KEK를 언랩하여 DEK와 파일에 액세스할 수 있도록 허용하는 CipherTrust Cloud Key Manager의 검증이 필요합니다.

## 주요 이점

워크로드와 애플리케이션을 클라우드로 마이그레이션하는 조직은 구글 워크스페이스와 같은 협업 제품군을 수시로 활용합니다. 원하는 장치로 어디서나 쉽게 액세스할 수 있는 엄청난 이점을 제공하는 동시에 외부 아이덴티티와 암호화를 추가함으로써 사용자가 암호 키를 제어할 수 있도록 지원하고 클라우드에 존재하는 중요한 기업 자산에 대한 개인정보 보호 및 보안 계층을 추가합니다.

탈레스는 독립적인 IDP, 인증 및 키 관리를 제공하는 유일한 보안 제공업체로서, 클라이언트 측 암호화를 통해 어떻게 구글 워크스페이스를 보호할 것인가에 대한 클라우드 보안 모범 사례를 충족할 수 있도록 지원합니다.

탈레스의 통합된 액세스 및 키 관리 솔루션은 다음과 같은 유형의 이점을 제공합니다.

- **보안:** 조직이 액세스 보안 및 키 관리를 자체적으로 운영함으로써 데이터 침해와 패널티의 위험을 줄일 수 있습니다.
- **원활한 배포:** 구글 워크스페이스를 통한 단일 벤더 통합이 빠르고 원활한 배포를 지원합니다.
- **우수한 사용자 경험:** 사용자가 구글 워크스페이스와 기타 클라우드 서비스 및 앱에서 SSO 기능을 이용할 수 있습니다.

## 주요 특징

### 클라이언트 측 암호화를 위한 아이덴티티 보호

STA는 독립된 제3자 IDP로서, 구글 워크스페이스에 사용자를 인증합니다. STA는 OIDC 통합을 통해 구글 워크스페이스 클라이언트 측 암호화를 위한 인증을 지원합니다.

### 구글 워크스페이스에 대한 인증 및 보안 액세스 강화

STA는 SAML 통합을 통해 구글 워크스페이스를 페더레이션하여 SSO(single-sign-on)를 지원하며, 사용자가 자신의 구글 서비스에 로그인할 때 적절한 수준의 인증을 실시합니다.

### 단순하면서도 강력한 인증

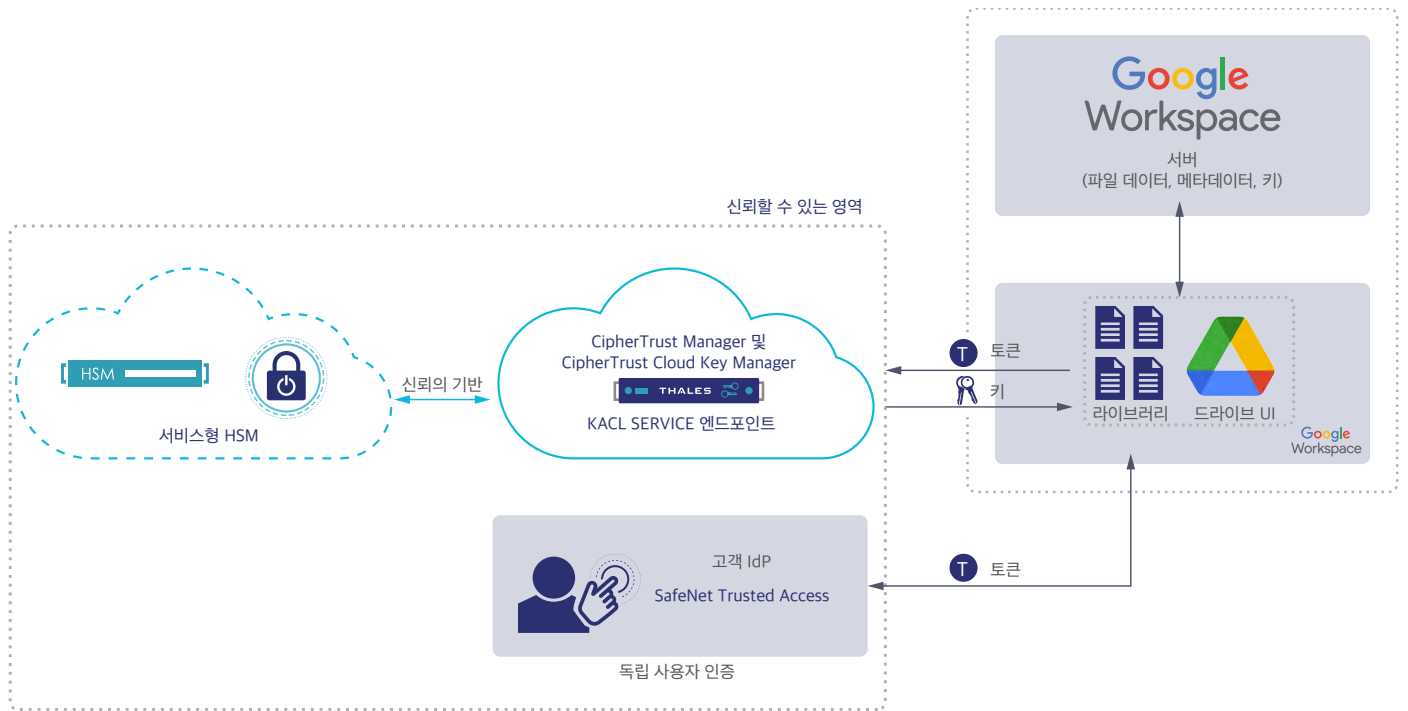
모든 리소스에 대해 강력하고 지속적인 인증, Single Sign-On 및 다단계 인증을 시행하는 선 인증 후 액세스 컨셉에 의해 제로 트러스트 보안 모델을 적용합니다. 인증 방식은 다음과 같습니다. FIDO, 하드웨어 토큰, 소프트웨어 토큰(OTP 앱), OOB(out-of-band, 대역 외) 푸시 인증, CBA(certificate-based authentication, 인증서 기반 인증), 패턴 기반 인증, SMS와 이메일을 통한 OOB, 상황 기반 인증.

### 간편하고 손쉬운 방식

예정된 기간 내에 기존의 자격증명을 사용하도록 재인증을 구성함으로써 보안을 저해하지 않고 사용자의 불편을 줄입니다.

### 구글 워크스페이스를 위한 키 관리

CipherTrust Cloud Key Manager는 외부 키 관리와 정책 제어 기능을 제공하여 오직 권한 있는 사용자만이 암호화된 문서에 액세스할 수 있도록 보장합니다.



## 구글 워크스페이스 클라이언트 측 암호화 소개

구글 워크스페이스 클라이언트 측 암호화(Google Workspace Client-side encryption)는 고객이 데이터의 기밀성을 강화하고 데이터 주권 및 규정준수에 관한 폭넓은 요건을 충족할 수 있도록 지원합니다. 고객은 암호화 키와 암호화 키에 액세스하기 위한 아이덴티티 서비스를 직접 관리할 수 있습니다. 사용자는 협업 기능을 계속 이용할 수 있고, 모바일 장치의 콘텐츠에 액세스하고 암호화된 파일을 외부에서 공유할 수 있으나, 구글은 고객 데이터를 해석할 수 없습니다.

## 구글 워크스페이스 소개

구글 워크스페이스는 모든 규모의 기업에게 연결, 생성 및 협업에 필요한 모든 것을 제공하는 통합 협업 및 커뮤니케이션 플랫폼입니다. 구글 워크스페이스에는 Gmail, Google Meet, Calendar, Drive, Docs, Sheets, Slides 등의 앱이 포함되어 있습니다. 자세한 정보는 [workspace.google.com](https://workspace.google.com)

## 탈레스 액세스 관리 소개

탈레스가 제공하는 업계 최고의 액세스 관리 및 인증 솔루션은 기업이 제로 트러스트 접근법을 통해 기업 IT와 웹 및 클라우드 기반 애플리케이션을 중앙형으로 관리 하고 보안 액세스 하도록 지원합니다. 기업은 정책 기반 조건부 액세스, 엄격한 SSO 및 범용 인증 방법을 활용하여 효과적으로 침해를 방지하고 클라우드로 안전하게 마이그레이션하며 규정준수 요건을 간소화할 수 있습니다.

## 탈레스 데이터 보안 소개

CipherTrust Data Security 플랫폼은 보안 팀이 멀티 클라우드 전략을 지원하는 과정에서 겪게 되는 여러 문제점을 완화하도록 설계된 클라우드 레디 제품 포트폴리오입니다. 이 플랫폼은 데이터 보안 및 암호화 키 관리 작업을 모두 처리하는 독보적인 솔루션을 다양하게 제공합니다. 이 플랫폼에는 CipherTrust Cloud Key Manager가 포함되어 있습니다.

## 탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 데이터 보안과 관련하여 점점 더 많은 결정적인 순간에 직면하게 됩니다. 그것이 암호화 전략 구축이거나, 클라우드 이전이거나, 규정 준수 요건 충족이 필요한 순간이거나, 그 어떤 경우여도, 탈레스는 당신의 디지털 전환을 안전하게 보호합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.