

## 탈레스의 엔드투엔드 암호화 솔루션: 정부 데이터 보호



# 목차

|          |                               |
|----------|-------------------------------|
| <b>3</b> | <b>정부 데이터 보호</b>              |
| 3        | 암호화의 필요성                      |
| 3        | 보호와 예방                        |
| <br>     |                               |
| <b>4</b> | <b>20여 개국 이상의 정부로부터 얻은 신뢰</b> |
| 4        | 성능을 저해하지 않으면서 데이터 보호 효과 극대화   |
| 4        | 정부 고객                         |
| <br>     |                               |
| <b>5</b> | <b>적합한 암호화 솔루션 선택</b>         |
| <br>     |                               |
| <b>6</b> | <b>엔드투엔드 암호화 솔루션</b>          |
| 6        | 탈레스 CN 시리즈 하드웨어 암호화 기기        |
| 6        | 탈레스 CV 시리즈 가상 암호화 기기          |
| 6        | Suredrop 암호화 파일 공유            |
| <br>     |                               |
| <b>7</b> | <b>탈레스 암호화 기기가 독보적인 이유</b>    |
| 7        | 최고의 성능                        |
| 7        | 높은 품질 보증                      |
| <br>     |                               |
| <b>8</b> | <b>네트워크에 구애받지 않는 암호화</b>      |
| 8        | 다기능성 및 편의성                    |
| 9        | 저비용, 고효율                      |
| <br>     |                               |
| <b>9</b> | <b>탈레스 소개</b>                 |

# 정부 데이터 보호



지방 정부 및 중앙 정부 기관은 다수의 민감 데이터를 보유하고 있으므로 사이버 보안은 어느 때보다 중요한 문제가 되고 있습니다.

시민의 개인 정보부터 국가 기밀에 이르기까지 모든 데이터를 보호하기 위해서는 거시적 접근이 필요한데, 그 중심에는 저장 데이터 및 전송 데이터 유출 방지/보호 솔루션이 있습니다.

지금까지는 실제 인프라와 가상 인프라를 조합한 예방 기술이 강조돼왔습니다. 그러나 지난 10년간의 시행착오에서 얻은 교훈이 있다면 데이터 유출 사고는 필연적이라는 사실입니다.

우발적 데이터 유출은 최근 몇 년간 소폭 감소했음에도 불구하고 여전히 전체 데이터 유출과 데이터 도난의 1/3을 차지하고 있습니다. 데이터 유출 사고의 주범은 악의를 품은 외부인, 즉 ‘해커’입니다. 2019년에 발생한 데이터 유출 사고의 원인 중 52%가 해킹, 28%는 악성 코드, 그리고 나머지 32~33%가 사회 공학적 수법(이른바, 피싱)이었습니다.

## 암호화의 필요성

가상화, 데이터 센터 및 클라우드 컴퓨팅 기술이 급격히 성장하면서 필요하면 언제 어디서든 고속/고가용성 데이터 네트워크를 통해 정보를 전송하는 경우가 점점 증가하고 있습니다.

해킹, 산업 스파이 활동, 심지어 사이버 테러 형태의 사이버 범죄 역시 증가하고 있습니다. 정보 보안 위협이 만연한 상황에 기업에게 저장 데이터와 전송 데이터의 무결성과 보안을 유지하는 일은 매우 중요한 일이 되었습니다.

회사 내에서조차 데이터의 안전을 보장받을 수 없습니다. 모든 기업은 공통 네트워크 액세스 방식으로 시스템 및 정보를 공유하며, 대다수 기업은 적게는 수 미터부터 수천 킬로미터까지 떨어져 있는 다수의 사무실을 운영하기도 합니다.

매일 사설 네트워크와 공용 네트워크를 통해 페타바이트 용량의 데이터를 전송하는 데는 광섬유 케이블이 사용됩니다. 광통신망은 여전히 가장 빠르고 안정적인 데이터 전송 방식으로 여겨지지만, 날로 정교해지고 저렴한 비용으로도 쉽게 접근 가능한 해킹 기술의 발전으로 인하여 점점 데이터의 보안도 위협받고 있는 실정입니다.

## 보호와 예방

강력한 방화벽이면 무단 네트워크 액세스를 막을 수 있다고 오해하는 기업이 많습니다. 유감스럽게도 사실은 그렇지 않습니다.

방화벽은 다양한 침입 또는 서비스 거부 공격을 감지하고 차단할 수 있지만, 방화벽 안팎의 물리적 악용에는 무용지물일 수 밖에 없습니다.

네트워크를 통해 전송되는 데이터를 보호할 수 있는 유일한 안전장치인 암호화입니다. 게다가 암호화 솔루션은 특정 네트워크 아키텍처에서 분리되며, 세계적으로 인정받는 보안 표준에 따라 인증 받습니다.

# 20여 개국 이상의 정부로부터 얻은 신뢰

인증받은 탈레스의 품질 보증 암호화 기기는 네트워크 성능을 저해하지 않으면서 고속 데이터 네트워크를 통해 전송되는 정부의 민감한 정보를 보호하는 데 애용되는 특수 하드웨어 제품입니다.

하드웨어 형태의 탈레스 암호화 기기는 여러 독립적인 테스트 기관의 인증을 받아 정부 부서와 기관에서도 사용되고 있습니다. 또한 탈레스 암호화 기기는 FIPS, Common Criteria, NATO로부터 정부 및 국방용으로 적합하다고 인증받았습니다.

인증의 일환으로 테스트 기관의 자체 실험실에서 다년간의 엄격한 테스트도 이뤄졌습니다. 이러한 인증을 받지 않은 제품은 정부의 데이터 네트워크에 설치될 수 없습니다.

이와 같은 인증과는 별도로, 정부와 국방부는 탈레스 암호화 기기에 대한 개념 증명 및 벤치마킹 테스트를 자체적으로 실시했습니다. 해당 테스트에서 탈레스 암호화 기기는 우수한 성적을 거뒀습니다.

무엇보다도, 정부와 국방 부문에 서비스(예: 클라우드 컴퓨팅 또는 데이터 센터 스토리지 서비스)를 제공하는 기업이 탈레스의 품질 보증 암호화 기기를 사용한다는 것은 정부 고객의 인증 조건을 충족할 수 있다는 뜻이기도 합니다.

이와 같이 신뢰할만한 인증을 취득한 탈레스 암호화 기기가 전 세계에서 가장 민감한 데이터를 보호하는 데 사용되며, 전 세계 정부 부서와 국방 담당 부서가 탈레스 암호화 기기를 선택하고 있습니다.

장기적인 데이터 무결성 및 보안 유지 외에도, 탈레스 암호화 기기는 다음과 같은 문제로부터 정부를 안전하게 보호합니다.

- 데이터 스니핑(이른바, '데이터 도청')
- 데이터 도용 또는 리디렉션
- 불량 데이터 입력
- 지적 재산 유출
- 개인정보 유출 또는 신원 도용
- 신뢰도 또는 평판 하락
- 재정적 손실 또는 과징금
- 준수 의무 위반
- 무고한 인적/기술적 오류

## 성능을 저해하지 않으면서 데이터 보호 효과 극대화

탈레스 암호화 기기는 네트워크 성능을 저해하지 않으면서 최고 수준의 보안을 지원합니다.

탈레스 암호화 기기를 사용하면 다른 '저급' 유사 제품과 달리 네트워크의 부담이 가중되거나 네트워크 회선의 불필요한 노출을 차단합니다.

20여 개국 이상의 정부는 필수적인 민감 데이터를 보호하기 위하여 다음과 같은 다양한 분야에 탈레스 암호화 기기를 사용하고 있습니다.

- 클라우드 컴퓨팅
- 빅데이터 수집 및 분석
- 데이터 센터 백업 및 재해 복구
- CCTV 네트워크

## 정부 고객

탈레스 암호화 기기는 네트워크를 통해 전송되는 많은 정부와 국방부의 데이터를 보호하는 데 사용됩니다.

탈레스 암호화 기기는 Common Criteria, NATO 또는 FIPS 인증을 요하는 다음과 같은 조직이나 환경에 사용되고 있습니다.

- 정부 기관 - 법 집행 기관, 서비스 기관, 규제 기관 등
- 국방 및 군사
- 정부 기관 및 부서 간의 데이터 공유
- 정부 통신망에 제공되는 통신사 네트워크 서비스
- 정부가 사용하는 클라우드 컴퓨팅 및 데이터 센터 서비스
- 사무실 간 및 사무실 내 데이터 통신 네트워크

# 적합한 암호화 솔루션 선택

다양한 네트워크 암호화 솔루션 간의 호환성이 부족하다는 것은 핵심 IT 인프라와 가상화된 WAN을 동시에 보호하려는 기업이 기술 선택에 보다 신중해야 한다는 의미입니다.

암호화 솔루션 제공업체를 선택할 때 모든 잠재적 용도까지 고려되어야 합니다. 모든 암호화 솔루션이 동일하게 설계된 것은 아니라는 사실 역시 염두에 두어야 합니다.

주요 데이터 보안 및 암호화 분석가는 견고하면서도 장기적(심지어 데이터의 유효 수명 이후까지)으로 데이터를 보호하는 네트워크 암호화 솔루션을 원한다면 '품질 보증' 솔루션을 선택할 것을 권장합니다.

암호화 기능이 내장된 네트워크 라우터/스위치 같은 이른바 '하이브리드' 암호화 기기나 (WAN 및 MAN 보안용이 아닌) MACSec 또는 그와 유사한 표준을 사용하는 기기는 '저급' 수준의 데이터 보호 기능만을 지원합니다.

반면에 탈레스 CN 시리즈 네트워크 암호화 솔루션은 세계 유수의 독립 테스트 기관으로부터 정부 보안 및 국방에 적합하다는 것을 인증받았습니다. 이 솔루션은 품질 보증 네트워크 데이터 보안 전용으로 특별히 설계되었습니다.

탈레스 네트워크 암호화 기기의 다음과 같은 4가지 필수 요소가 인증 기관을 통해 검증되었습니다.

- 네트워크 데이터 암호화 전용 변조 방지 하드웨어
- 최첨단 암호키 관리, 클라이언트 측 키 저장소 보호 기능
- 엔드투엔드 인증 방식 암호화
- 표준 기반의 암호화 알고리즘

실시간 데이터 전송 환경에서 지연 시간은 매우 중요한 문제입니다. 네트워크 암호화 인터페이스 카드를 기존 스위치에 추가하는 것이 그럴듯한 선택지처럼 보일 수 있으나, 레이어 2 전용 기기보다 지연 시간도 길고 처리 성능 역시 떨어집니다.

네트워크 암호화 인터페이스 카드를 사용하면 네트워크 경로 내내 동일한 솔루션 제공업체를 사용해야 하며, 모든 '홉'에서 매번 데이터를 해독했다 다시 암호화해야 합니다.

이런 상황은 보안 위험과 중대한 키 관리 문제를 야기합니다. 반면에 전용 어플라이언스를 사용하면 스위치 제조업체와 관계없이 네트워크 경로 내내 데이터가 암호화된 상태를 유지할 수 있습니다.

네트워크 암호화 인터페이스 카드를 사용하는 경우 암호화 기기의 수명은 호스트 네트워크 기기에 따라 달라지며, 스위치를 바꾸면 암호화 기기 역시 교체해야 합니다.

대부분의 최신 인프라는 다양한 네트워크 레이어(일반적으로 레이어 2, 3 및 4 요소)로 구성됩니다. 따라서 기업은 가급적이면 레이어에 구애받지 않는 암호화 기술을 지원하는 솔루션 제공업체를 선택해야 합니다.

탈레스의 CV 시리즈 가상 어플라이언스는 동시 다중 레이어 암호화와 더불어, DPDK를 통해 최대 5Gbps의 속도를 제공합니다.

탈레스의 가상 어플라이언스는 CN 시리즈 하드웨어 암호화 기기와 마찬가지로 P2P부터 허브 앤 스포크(Hub & Spoke)와 완전 메시형 네트워크에 이르기까지 모든 토폴로지를 지원합니다.

# 엔드투엔드 암호화 솔루션

## 탈레스 CN 시리즈 하드웨어 암호화 기기

CN 시리즈 네트워크 암호화 기기는 코어 IT 및 통신 네트워크 인프라에 인증받은 품질 보증 데이터 보호 기술을 지원합니다.

모든 CN 시리즈 암호화 기기는 공통 암호화 플랫폼을 공유하며 서로 완벽하게 호환되고 연동됩니다.

CN 시리즈 하드웨어 암호화 기기는 일반적인 속도인 10Mbps부터 100Gbps에 달하는 초고속 대역폭에 이르기까지 모든 속도의 네트워크를 통해 전송되는 민감 데이터를 보호하는 데 사용됩니다.



### CN4000

10Mbps, 100Mbps 및 1Gbps 대역폭 속도를 지원하는 '옥외' 네트워크 회선(예: CCTV) 보안용 소형 폼 팩터(데스크탑) 암호화 기기입니다.



### CN6000

1Gbps~10Gbps 대역폭 속도를 지원하는 비즈니스 크리티컬 애플리케이션용 랙 장착형 고속 암호화 기기입니다.



### CN9000

최대 100Gbps의 속도를 통해 대용량 데이터 전송을 지원하는 초고대역폭, 랙 장착형 암호화 기기입니다.

## 탈레스 CV 시리즈 가상 암호화 기기

CV1000 가상 암호화 기기는 대규모 및 가상 광역 네트워크에 강력하고 효과적인 데이터 암호화를 지원합니다.

엔드포인트를 수천 개까지 확장할 수 있는 CV 시리즈 가상 암호화 기기는 신뢰할만한 탈레스 암호화 플랫폼의 소프트웨어 애플리케이션입니다. 이 제품은 레이어에 구애받지 않으면서 전송 속도가 최대 5Gbps(DPDK 사용)인 네트워크의 데이터를 비용면에서 경제적으로 보호합니다.

모든 x86 하드웨어에서 실행되는 VNF(Virtualised Network Function)인 CV 시리즈 가상 암호화 기기는 탈레스 CN 시리즈 하드웨어 암호화 기기와 완벽하게 연동되며, FIPS 호환 기술을 기반으로 합니다.

## Suredrop 암호화 파일 공유

SureDrop은 널리 사용되는 박스형 애플리케이션의 편리한 파일 공유 방식에 엔드투엔드 암호화 보안 기능과 완벽한 데이터 위치 제어 기능까지 견비하고 있습니다.

또한 SureDrop은 사용자에게 맞춤형 온프레미스 솔루션의 복원성과 서비스 제공업체 관리형 솔루션의 유연성 중 선택할 수 있는 옵션을 제공합니다.

보호받지 못하는 외부 사용자와 문서를 공유하는 데 고질적으로 수반되는 위험을 우려하는 정부 기관과 서비스 제공업체가 SureDrop을 주로 사용합니다.

SureDrop은 안전한 파일 공유를 만끽할 수 있는 새로운 방법을 제시합니다. 요컨대, SureDrop은 웹을 통해 민감한 정보와 기밀 정보를 자주 공유해야 하는 대기업과 정부 기관의 요구에 부합하는 서비스를 제공합니다.

또한 SureDrop은 기업에서 주로 사용되는 Active Directory 사용자 인증 방식을 지원한다는 장점도 있습니다.

# 탈레스 암호화 기기가 독보적인 이유



## 최고의 성능

### 빠른 속도

많은 유사 제품 중에서 탈레스 암호화 기기가 단연 돋보이는 이유로는 업계 최고의 성능을 손꼽을 수 있습니다.

탈레스 암호화 기기는 10Mbps, 100Mbps, 1Gbps, 10Gbps 또는 100Gbps의 속도를 기준으로 한 성능 비교 테스트에서 번번이 경쟁사 제품을 압도하였습니다.

탈레스 암호화 기기는 탁월한 암호화 속도와 사실상 전무한 데이터 오버헤드 및 지연 시간을 자랑하므로 매우 엄격한 네트워크 환경에 사용하기 적합합니다.

### 극도로 짧은 지연 시간

탈레스 고속 암호화 기기는 전이중 모드에서 패킷 손실 없이 최대 회선 속도(99.99%)로 작동합니다.

지연 시간은 패킷 크기(10Gbps에서 단위당 2마이크로초 미만)의 영향을 받지 않으므로 최상의 처리 속도가 유지되고 사실상 프로토콜 오버헤드가 전무합니다.

무엇보다도 FPGA(Field Programmable Gate Array) 기술을 사용하기 때문에 우수한 성능은 안정적으로 계속 유지됩니다.

### 제로 임팩트

탈레스 암호화 기기는 네트워크 대역폭과 지연 시간뿐만 아니라, 네트워크 운영과 관리에 끼치는 영향도 매우 미미합니다.

탈레스 암호화 기기가 영향을 미치는 곳은 사용자 네트워크뿐입니다. 다른 기기로 교체하거나 네트워크를 재구성할 필요도 없습니다. 이러한 이유로 탈레스 암호화 기기는 네트워크 엔지니어들에게 큰 인기를 누리고 있습니다.



## 높은 품질 보증

### 격이 다른 인증

탈레스 CN 시리즈 암호화 기기는 동종 제품 중 유일하게 다수의 기관의 인증을 받았기 때문에 전 세계 정부와 국방부로부터 신뢰를 받고 있습니다.

수년에 걸쳐 진행된 엄격한 테스트는 정부 및 기업 고객에게 확실한 믿음을 줍니다. 탈레스 CN 시리즈 암호화 기기는 FIPS, Common Criteria, NATO의 인증을 받았습니다.

지난 20년간 탈레스 R&D 센터는 비교 불가능한 인증을 획득하기 위하여 주력해왔습니다. 고객은 철저하고 지속적인 테스트 기관의 제품 평가에서 입증된 이점을 신뢰합니다.

### 최고의 암호키 관리

모든 탈레스 제품에는 최첨단 암호키 관리 기술이 채택됩니다. 고객의 암호키는 해당 고객만 보유하고 액세스할 수 있으며, 온프레미스에 안전하게 암호화되고 보관됩니다.

### 솔루션 무결성

탈레스 암호화 기기는 라우터 기반의 네트워크 데이터 암호화나 이른바 ‘하이브리드’ 암호화 기기 같은 ‘저급’ 솔루션과 달리, 최상의 솔루션 무결성을 보장합니다.

탈레스의 품질 보증 암호화 솔루션에는 변조 방지 전용 하드웨어를 탑재하고, 표준 기반(AES256) 암호화 알고리즘을 사용하여 빈틈없는 엔드투엔드 인증 방식 암호화를 지원합니다.



# 네트워크에 구매받지 않는 암호화

많은 기업이 비즈니스 애플리케이션 및 통신 서비스를 지원하는 데 여러 데이터 네트워크 레이어 프로토콜(레이어 2, 3 및 4)을 활용합니다. 탈레스는 이를 염두에 두고 자체적으로 네트워크에 구매받지 않는 암호화(Network Independent Encryption) 기술을 개발했습니다.

네트워크 레이어에 구매받지 않는 고급 암호화 기술은 정책 기반 동시 다중 계층 암호화를 실현합니다.

무엇보다도, 보호받는 데이터가(예를 들어, 레이어 2 이더넷부터 레이어 3 IP 네트워크 대상에 이르기까지) 다양한 네트워크 레이어를 통과하므로 강력한 엔드투엔드 암호화가 보장됩니다.



## 다기능성 및 편의성

### 암호화 민첩성

모든 탈레스 암호화 기기는 맞춤형 암호화와 FPGA 기반의 유연성을 기반으로하는 완벽한 호환성과 연동성을 아우르는 개념인 '암호화 민첩성(Crypto-agility)'을 특징으로 합니다. 일부 탈레스 암호화 기기는 장기적 관점의 데이터 보안을 위해 Quantum Key Distribution(Quantum Cryptography)과 Quantum Random Number Generation을 지원합니다.

### 모든 프로토콜 지원

탈레스 CN 시리즈 암호화 기기는 가장 폭넓은 기능들을 자랑합니다. 10Mbps~100Gbps의 속도에서도 기능을 발휘할 수 있고, 레이어 2 캐리어 이더넷 WAN 및 MAN 네트워크용으로 설계됐으며, 모든 레이어 2 프로토콜(Ethernet, Fibre Channel, SONET/SDH, LINK)에 대하여 지원합니다.

### 모든 토폴로지 지원

탈레스 CN 암호화 기기는 P2P(Point-To-Point), P2MP(Point-To-MultiPoint), 완전 메시형 네트워크 토폴로지에서 작동합니다. 특히 탈레스 CN9000은 MP2MP(MultiPoint-To-MultiPoint) 토폴로지를 지원하는 업계 유일의 100Gbps 암호화 기기입니다.

### 맞춤식 암호화

탈레스 CN 암호화 기기는 표준 기반의 AES256 및 128비트 알고리즘 외에도, 맞춤형 알고리즘(BYOC 및 BYOE)을 지원합니다.

### 사용 용이성

'한 번만 설정하면 끝'인 편의성과 네트워크 투명성은 탈레스 제품의 기본 요소입니다. 탈레스 암호화 기기는 편리한 구현, 운영, 관리를 보장합니다. 모든 탈레스 암호화 기기는 완벽하게 자동화된 키 관리 기능을 갖추고 있습니다. 또한 자동 네트워크 탐색 및 연결 기능도 지원합니다.

### 연동성

동일한 Layer 2 네트워크 프로토콜을 지원하는 탈레스 암호화 기기는 완벽하게 서로 연동됩니다. 모든 탈레스 CN 모델은 이전 모델과 호환됩니다.

### 로컬 또는 중앙 집중식 관리

직관적인 탈레스 CM7 관리 소프트웨어를 통해 로컬로 또는 원격으로 구성 가능하며, 이 소프트웨어는 X.509 인증서에 서명하고 배포하는 방식으로 중앙화된 정책으로 관리합니다.





## 저비용, 고효율

### 적합성

모든 탈레스 CN 암호화 기기는 최대 유선 속도로 작동하며, 네트워크 성능을 극대화하고, '한 번만 설정하면 끝'인 단순하면서도 간편한 관리가 가능합니다.

기업 투자 사례에서 입증됐듯, 저렴한 가격에 현혹되어 저급 솔루션을 구매하면 장기적으로는 큰 비용이 발생하게 됩니다.

열악한 비즈니스 상황과 TCO 조건을 맞추는 것에 급급하여 저렴한 저급 솔루션을 선택해서는 안됩니다.

### 경제성

탈레스 암호화 기기는 네트워크 대역폭 절약, 손쉬운 관리, 안정성을 겸비하고 있어 총소유비용을 절약하는 데 이상적입니다.

긴 수명, 상호운용성, 이전 모델과의 호환성, 설치 및 관리 비용 최소화 및 솔루션 유연성은 빠른 투자 수익으로 이어집니다.

그 밖의 비용 이점으로는 적은 전력 소비량, 최소한의 랙 공간 사용, 랙 공간과 에너지 절약의 시너지 효과로 발생하는 효율성이 있습니다.

### 안정성

99.999%의 가용성을 보장하고, 국제 안전 및 환경 보호 기준에 부합합니다. 탈레스의 모든 캐리어급 랙 장착형 암호화 기기는 핫스왑 방식을 지원하며, 팬과 전원 공급 장치 같은 암호화 기기 소모품이 이중으로 구성되어 있어 네트워크 전송 데이터 암호화 작업의 가용성이 한층 더 높아집니다.

하이브리드 암호화 기기나 여타 저급 솔루션과 달리, 탈레스 암호화 기기는 네트워크 가용성에 영향을 미치지 않습니다.

### 유연성

탈레스 암호화 기기는 FPGA 기술을 사용하여 운영상의 유연성을 극대화합니다. 탈레스 암호화 기기는 고객별 조건을 충족하도록 최적화된 고속 데이터 암호화 솔루션입니다.

이러한 유연성 덕분에 고객의 필요 조건이 변경될 경우 즉시 업그레이드를 지원하여 지속적인 운영 간소화를 가능케함으로써 탈레스 제품에 대한 고객의 투자를 보호해 드립니다.

## 탈레스 소개

개인정보를 중요시하는 기업들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스의 보안 솔루션을 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션



#### 문의

사무소 위치 및 연락처 목록은 [cpl.thalesgroup.com/ko/contact-us](https://cpl.thalesgroup.com/ko/contact-us)에서 확인하실 수 있습니다.

> [cpl.thalesgroup.com](https://cpl.thalesgroup.com) <

