THALES

451 Research®

2018

# 탈레스 데이터 위협 보고서

## 암호화 및 데이터 보안 트렌드

**한국판**

개요

#2018DataThreat

## 소개

### 디지털 트랜스포메이션은 IT 팀에 엄청난 혼란을 일으키고 있을 뿐만 아니라 데이터 보안에 대한 새로운 접근방식을 요구하고 있습니다.

디지털 트랜스포메이션은 제품과 서비스의 규모를 확장하고 효율성을 향상할 수 있도록 해주며, 성장과 수익성을 지원하는 새로운 비즈니스 모델들을 가능하게 만들어 줍니다. 디지털 기술이 가진 모든 잠재력을 활용함으로써 국내 기업들은 이러한 기회를 적극 포용하고 있습니다. 그러나 기술 구현을 서두르다 보면 민감 데이터의 보안이 위험에 처할 수 있습니다.

이러한 변혁을 추진하기 위해 많은 기업이 클라우드, 빅데이터, IoT(사물인터넷), 컨테이너, 모바일 결제 및 블록체인 기술을 도입한 것으로 나타났습니다. 클라우드는 이제 보편적으로 사용되고 있으며, 구현된 다수의 클라우드 서비스를 어떻게 안전하게 사용하고 관리할 것인가에 대한 새로운 문제가 야기되고 있습니다. 빅데이터의 사용률은 현재 99%에 달하며, 블록체인, 모바일 결제, IoT의 도입률도 모두 90%를 상회합니다. 응답자의 95%가 이러한 환경 내에서 민감데이터를 사용하고 있다고 대답했습니다. 이러한 높은 도입률은 데이터 보안의 중요성을 한층 더 부각시켜줍니다. 각 환경에는 고유한 데이터 보안 문제가 존재합니다. 또한, 기업은 국제적인 규제는 물론 개인정보보호법(PIPA)처럼 개인정보를 사용하는 모든 곳에 적용되는 엄격한 국내의 규제요건을 충족해야만 합니다.

#### 디지털 트랜스포메이션은 데이터 보안에 대한 새로운 접근방식 필요

**95%** 는 **민감 데이터**에 디지털 트랜스포메이션 기술을 사용하고 있음 (클라우드, 빅데이터, IoT, 컨테이너, 블록체인 또는 모바일 결제)

#### 높은 수준의 도입률로 복잡성 가중

**100%** 일반적인 클라우드 사용

**99%** 빅데이터 사용

**95%** IoT 구현

**93%** 모바일 결제 사용 중 또는 사용 예정

**92%** 블록체인 프로젝트 구현 또는 구현 중

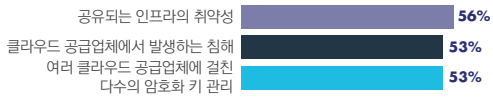
#### 멀티 클라우드 사용으로 인해 추가적인 리스크 발생

**66%** **2곳 이상의 IaaS** 공급업체 사용

**68%** 10개 이상의 **SaaS 애플리케이션 사용**

**71%** 2개 이상의 **PaaS** 환경 사용

#### 클라우드 컴퓨팅과 관련된 3대 우려사항




#### 긍정적인 소식

**올해 안에 데이터 보안 기술 구현 예정**

**52%** HSMs

**48%** BYOK (Bring Your Own Key) 암호화

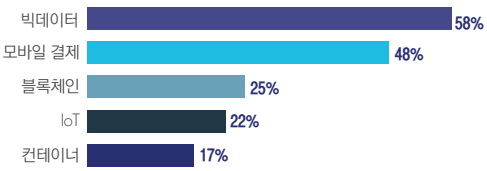
**44%** 클라우드에서의 암호화

**41%** 클라우드 암호화 게이트웨이 또는 클라우드 액세스 보안 브로커(CASB)

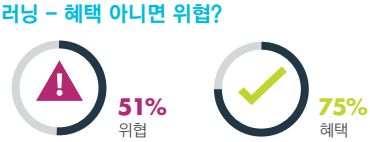
#### 디지털 트랜스포메이션 기술로 인해 리스크가 증가하고 있습니다.

#### 디지털 트랜스포메이션에서는 많은 양의 민감 데이터가 사용됩니다.

**디지털 트랜스포메이션에서는 많은 양의 민감 데이터가 사용됩니다.**




#### 머신 러닝 – 혜택 아니면 위협?

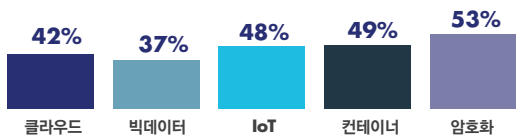


**51%** 위협

**75%** 혜택

#### 암호화는 데이터 보안 문제를 해결하는데 핵심입니다.

#### 암호화는 디지털 트랜스포메이션과 기존 방식의 데이터 보안을 지원합니다.




#### 올해 계획된 4가지 데이터 보안 툴 중 3가지는 암호화 기술임

**61%** 데이터 마스킹

**48%** 다요소 인증

**45%** 클라우드에서의 암호화

**45%** 토큰화


95%
"민감 데이터와 함께 디지털 트랜스포메이션 기술 사용(클라우드, 빅데이터, IoT 컨테이너, 블록체인 또는 모바일 결제)"
+6.5%
78%
CTMX
FTR
CSCO
CHK
AAPL
PRTO
AMZN
TSLA
AVGO
SIRI
0.45
-0.23
-2.34%
-1.01
-1.89%
0.02
-0.65

## 디지털 트랜스포메이션은 데이터 보안에 대한 새로운 접근방식을 요구합니다.

디지털 트랜스포메이션은 데이터 위협의 주요 원동력으로 진화해 왔습니다. 클라우드 및 SaaS 애플리케이션, 빅데이터, IoT, 컨테이너, 모바일 결제 및 블록체인 기술의 전반적인 도입 또한 보안 위협을 증대시킵니다. 이러한 기술들은 상대적으로 생소하고, 각 환경에서 데이터를 보호하는데 고유한 접근 방식이 요구되며, 구현의 규모가 방대하기 때문입니다. 이뿐만 아니라, 95%의 응답자들은 새로운 비즈니스 모델 지원, 비용 절감, 포괄적인 데이터세트 분석, 협업, 핵심 정보의 저장 등을 위해 이러한 환경에서 민감 데이터를 사용할 것이라고 대답했습니다.

디지털 트랜스포메이션에 가장 광범위하게 사용되는 기술은 클라우드(100%)와 빅데이터(99%)였습니다. 90% 이상의 기업은 올해 안에 IoT, 컨테이너, 모바일 결제 및 블록체인 기술을 구현할 예정인 것으로 나타났습니다. 민감 데이터의 사용은 이러한 새로운 기술의 구현에 내재한 문제를 한층 더 복잡하게 만듭니다.

"IT 보안 예산이 증가한 가장 큰 이유는 클라우드의 사용 증가 때문입니다."

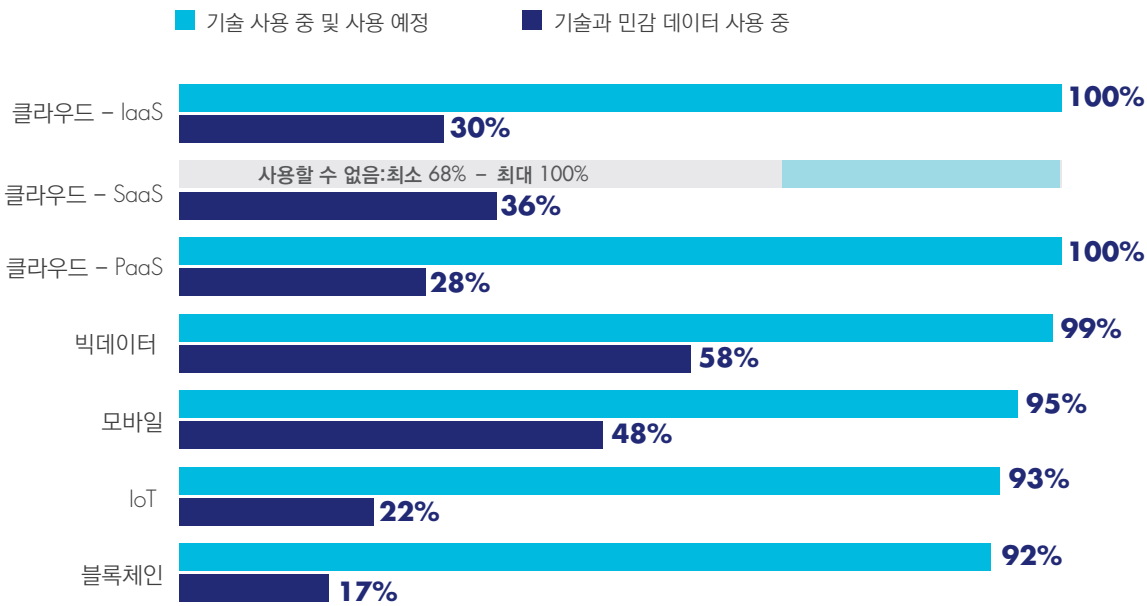
—GARRETT BEKKER, 451 RESEARCH 정보 보안 수석 분석가 &
**2018 탈레스 데이터 위협 보고서 저자**

### 디지털 트랜스포메이션 이니셔티브는 많은 민감 데이터를 사용합니다.

**95%** **민감 데이터**에 디지털 트랜스포메이션 기술 사용
(클라우드, 빅데이터, IoT, 컨테이너, 블록체인 또는 모바일 결제)

**47%** IT 보안 예산 증가를 부추기는 가장 큰 요인은 **클라우드 컴퓨팅의 도입**

### 디지털 트랜스포메이션 기술과 민감 데이터의 사용률 및 구현 수준



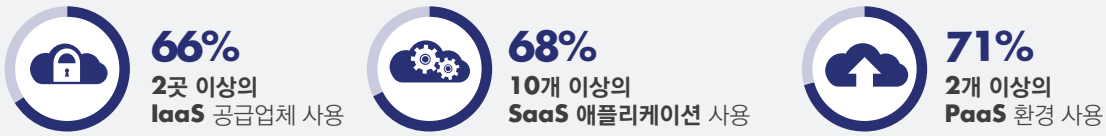
## 멀티 클라우드 운영이 야기하는 주요 우려 사항

66%의 기업은 10개 이상의 SaaS(서비스로서의 소프트웨어) 서비스를 사용하고 있으며, 66%는 2개 이상의 IaaS(서비스로서의 인프라)를, 71%는 2개 이상의 PaaS(서비스로서의 플랫폼)를 사용하고 있는 것으로 파악되었습니다. 이러한 수준의 클라우드 사용은 혁신과 효율성 향상을 지원하지만, 데이터 보안의 측면에서 대가가 따릅니다. 다양한 환경에서 데이터를 보호하고 통제를 유지하려면 고유한 요구사항이 생겨납니다. 이로 인해 야기되는 복잡성 수준으로 그 대가를 가늠할 수 있습니다.

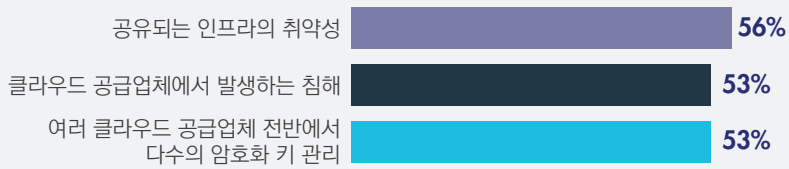
기존 데이터센터의 경우, 데이터는 건물 내에서 물리적으로 보안이 될 뿐 아니라, 구현 툴들의 기반이 되는 인프라와 네트워크도 조직이 직접적으로 통제를 했습니다. 그러나, IaaS의 경우, 각 구현 서비스와 환경에 따라 특별한 데이터 보안 계획을 수립하고 이를 정책, 운영 방식 및 툴로 시행해야 합니다. SaaS와 PaaS 환경은 상황이 좀 더 복잡합니다. 이러한 환경에서는 대부분, 데이터가 저장되거나 보호되는 방법을 조직이 통제할 수가 없습니다. AWS S3 스토리지 버킷 또는 Salesforce 구현처럼 데이터 보안 통제가 가능한 일부의 경우, 암호화 키 관리와 액세스 통제는 새로운 전문지식과 툴이 요구되는 새로운 과제가 됩니다. 여러 환경의 암호화 기술들을 통합 관리하여 이러한 복잡성을 감소시켜 주는 제3자 제품이나 서비스가 시중에 나와 있긴 하지만, 아직까지 널리 인정 받지는 못하고 있습니다. 조직들인 이러한 제품이나 서비스가 필요해질 것입니다. 보안의 기본 원칙은 '키를 통제하는 자가 데이터를 통제한다'라는 것입니다. 암호화 – 로컬 또는 클라우드 환경에서 관리되는 원격 암호화 키 제어가 필요합니다.

> "헛점이 많은 네트워크가 증가하고 외부 리소스(특히 SaaS, PaaS, IaaS)의 사용이 늘어나면서 기존의 엔드포인트와 네트워크 보안만으로는 더 이상 충분하지 않게 되었습니다."
>
> —GARRETT BEKKER, 451 RESEARCH 정보 보안 수석 분석가 & **2018 탈레스 데이터 위협 보고서 저자**

**멀티 클라우드 사용으로 인해**




**Top three concerns with cloud computing**




**긍정적인 소식**

오늘날 많은 기업들이 데이터 보안 기술을 구현하고 있습니다.

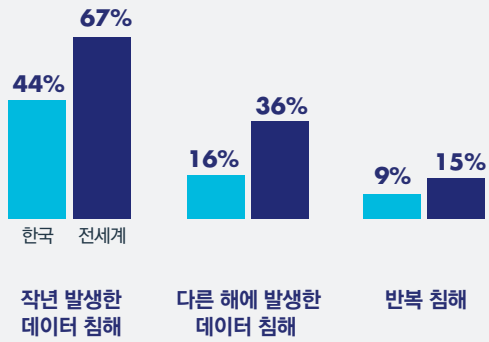
## 거의 절반에 가까운 국내 기업이 이미 데이터 침해를 경험

한국은 데이터 프라이버시와 정보 보안을 매우 심각하게 여깁니다. 6년째를 맞고 있는 개인정보보호법(PIPA)은 세계에서 가장 포괄적이고 엄격한 개인정보 보호 규제 중 하나로, 위반 시에는 고액의 벌금형과 징역에 처해질 수 있습니다. 이뿐만 아니라, 1년 전에는 데이터 보호 및 개인정보 요구사항을 불이행하는 경우 더 엄중한 처벌이 내려지도록 하는 규정이 생겼습니다.

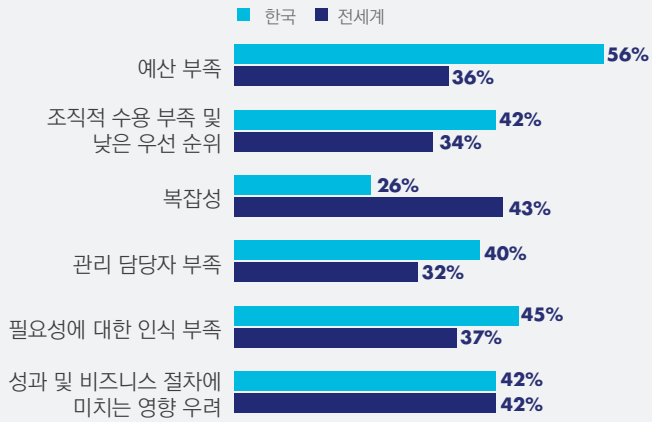
오늘날 국내 기업들은 이러한 매우 엄격하고 어쩌면 가혹할 수도 있는 데이터 보호 환경에서 비즈니스를 수행해야 합니다. 이러한 환경에서도, 설문조사에 참여한 IT 보안 담당자들의 거의 절반에 해당하는 44%는 자사가 데이터 침해를 경험한 적이 있다고 대답했습니다. 데이터 침해 3건 중 1건은 작년(16%)에 발생했으며, 9%의 기업은 작년뿐 아니라 그 이전에도 데이터 침해를 경험했다고 밝혔습니다.

이러한 수치들이 우려스럽긴 하지만, 국내의 조직들은 다른 국가의 조직들보다 침해율이 낮습니다. 아마도 엄격한 규제준수 체계가 구축되어 있는 탓인 듯 합니다.

**데이터 침해 발생률 국내 vs. 전세계**




**데이터 보안의 구현을 가로막는 장애물로 인지**




그러나, 설문조사 결과는 긍정적인 측면도 보여주었습니다. 이러한 위협에 대응하기 위해 기업들은 IT 보안 예산을 늘리기 시작했습니다. 예산 부족이 데이터 보안을 구현하지 않거나 예산을 늘리지 않는 가장 큰 이유(54%)이지만, 76%는 IT 보안 예산을 늘릴 예정이고, 12%는 올해 예산을 대폭 증가할 것이라고 대답했습니다.

> "데이터 보호의 추가적인 계층을 위해 사용과 구현의 복잡성을 감소시켜 주는 자동화, 서비스 기반의 구현, 플랫폼을 제공하는 데이터 보안 툴 세트를 선택해야합니다."
>
> —GARRETT BEKKER, 451 RESEARCH 정보 보안 수석 분석가 &
> **2018 탈레스 데이터 위협 보고서 저자**

"한국은 세계에서 데이터 침해 사고 발생율이 가장 낮은 편에 속합니다. 작년에 침해 사고를 경험했다고 밝힌 조직들은 16%로 전세계 평균인 36%의 절반도 되지 않습니다."

## 조직들은 데이터 보호 방식을 바꿀 필요가 있습니다.

### 기업들은 데이터를 효과적으로 보호해주지 않는 툴에 가장 많은 예산을 소비한 것으로 나타났습니다.

응답자들은 데이터 보호를 위해 특별히 설계된 방어 체계가 가장 효과적인 툴임을 확실하게 인지하고 있습니다. 응답자의 68%가 저장 데이터 보호를 매우 또는 극도로 효과적이라고 대답하여, 저장 데이터 보호가 데이터 보호에 가장 효과적인 툴인 것으로 나타났습니다. 그러나, 예산 증가에서 저장 데이터를 위한 보안 툴은 우선 순위가 그다지 높지 않습니다. 실제로, 대규모 데이터 스토어를 보호하는데 가장 효과가 있는 저장 데이터 보호는 예산 규모 증가에서 우선 순위가 거의 최하위(35%)였습니다. 분석과 상관 관계 툴만이 이보다 낮은 34%였습니다.

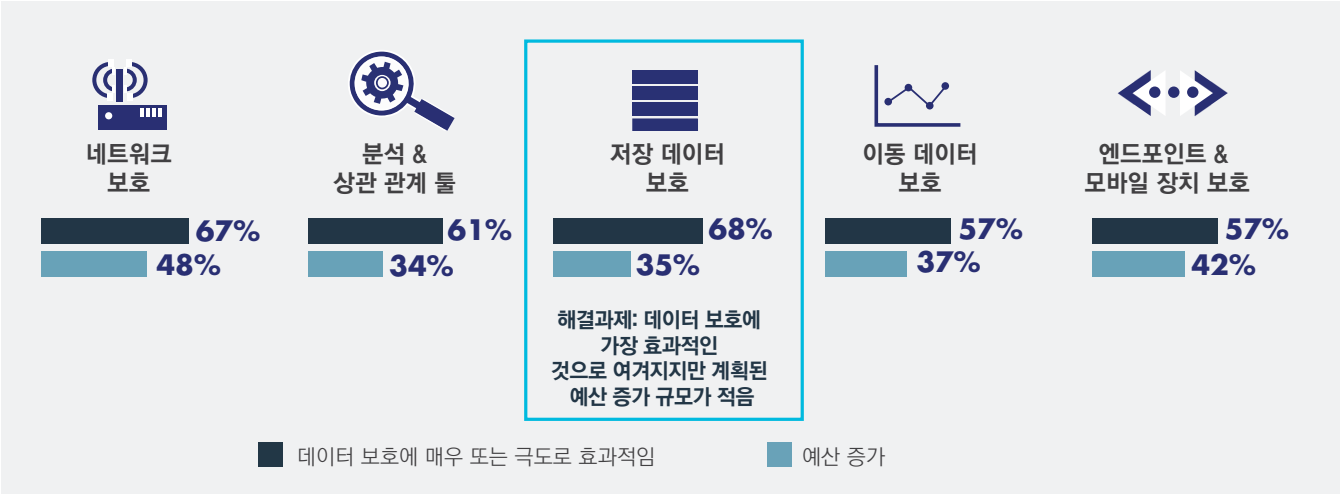
동시에, 네트워크(48%)와 엔드포인트(42%) 보호에 가장 많은 예산이 집행되고 있었습니다. 클라우드 컴퓨팅 때문에 이러한 툴들의 관련성이 점점 사라지고 있고 데이터 침해를 위해 고안된 공격에 완전히 속수무책임에도 불구하고 말입니다. 범죄형 해커들이 스피어 피싱과 제로데이 취약점 공격을 쉽게 사용할 수 있는 현실에서, 네트워크 및 엔드포인트 기반의 보안 통제로 네트워크 침입을 차단한다는 것은 거의 불가능한 일입니다. 또한 응답자들은 데이터세트를 중심으로 추가적인 보호 계층을 제공하는 가장 효과적인 솔루션은 보안 통제라는 점을 인지하고 있습니다. 저장 데이터와 이동 데이터 보안 툴은 공격 가능 영역을 감소해주며, 대용량 데이터세트를 둘러싸고 진행 중인 공격을 신속하게 파악 및 차단하는데 필요한 정보를 제공할 수 있습니다.

"IT 보안 툴 세트의 재우선순위화가 필요합니다."

"헛점이 많은 네트워크가 증가하고 외부 리소스(특히 SaaS, PaaS, IaaS)의 사용이 늘어나면서 기존의 엔드포인트와 네트워크 보안만으로는 더 이상 충분하지 않게 되었습니다."

"데이터 보안은 첨단 기술 환경 내에 존재하는 알려진 또는 알려지지 않은 민감 데이터에 대한 보호를 향상시켜 줍니다."

—GARRETT BEKKER, 451 RESEARCH 정보 보안 수석 분석가 &
**2018 탈레스 데이터 위협 보고서 저자**



## 암호화는 데이터의 위치에 상관 없이 민감 데이터 보호에 핵심적인 툴입니다.

### 데이터센터, 클라우드, 빅데이터 및 민감 정보가 사용 또는 저장되는 모든 곳에서 데이터 보호

긍정적인 소식 국내 기업들은 암호화 기술이 데이터 보호에 가장 효과적이라고 인지하고 있으며, 예산 비중이 낮긴하지만 데이터 보호를 위한 암호화를 꽤 높은 수준에서 구현 중이라고 대답했습니다. 기업들이 올해 구현 예정인 주요 데이터 보안 툴 중 3가지는 암호화 기술(데이터 마스킹, 클라우드 암호화, 토큰화)입니다. 또한 32%는 이미 클라우드 환경에서 일부 암호화를 사용하고 있었습니다. 디지털 트랜스포메이션의 사용을 확장하는데 필요한 IT 보안 툴로는 암호화와 액세스 통제가 상위를 차지했습니다. 마지막으로, 53%는 전세계 데이터 프라이버시 및 데이터 주권 요구사항을 충족하기 위해 데이터 암호화를 계획하고 있었습니다.

**올해 계획된 데이터 보안 툴 4개 중 3개** (미구현)**:**

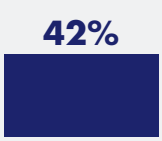

**61%**
데이터 마스킹

**48%**
다요소
인증

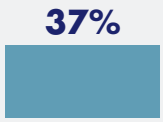
**45%**
클라우드에서의
암호화

**45%**
토큰화

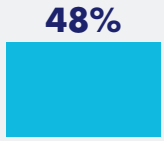
**디지털 트랜스포메이션을 추진하는데 필요한 암호화**



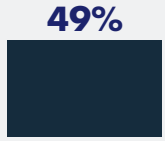

**클라우드:**
암호화는 클라우드
사용 확대를 위한
상위 3개
툴 중의 하나임




**빅데이터:**
기반 시스템 및
연산 노드를 위한
시스템-레벨 암호화 및
액세스 제어는
빅데이터
사용 확대에 필요




**IoT:**
보안 인증 암호화 기술은
IoT 사용 확대를 위한
상위 3개
툴 중 하나임




**컨테이너:**
암호화는
컨테이너
활용 증가 지원

**53%**
암호화는 일반 데이터 보호
규정(GDPR)과
같은 글로벌 개인정보
보호 규제 충족을 위한
최고의 툴임

**68%**
의 응답자들은 데이터베이스 및
파일 암호화를 현재 구현 중

"한국의 클라우드 도입률은 미국 보다 낮지만, 보안 예산을 늘리는 가장 큰 이유로 클라우드 사용 증가를(47%) 꼽았습니다. 이는 세계 평균(39%) 보다 훨씬 더 높은 수준입니다."

"헛점이 많은 네트워크가 증가하고 외부 리소스(특히 SaaS, PaaS,IaaS)의 사용이 늘어나면서 기존의 엔드포인트와 네트워크 보안만으로는 더 이상 충분하지 않게 되었습니다." (추후 개조 보다 쉽기 때문에) 초기 개발의 일부로 구현되는 경우, 데이터 보안은 첨단 기술 환경 내에 존재하는 알려진 또는 알려지지 않은 민감 데이터에 대한 보호를 향상해줍니다."

"데이터 보호의 추가적인 계층을 위해 사용과 구현의 복잡성을 감소해주는 자동화, 서비스 기반의 구현, 플랫폼을 제공하는 데이터 보안 툴 세트를 선택해야 합니다."

—Garrett Bekker, 451 Research 정보 보안 수석 분석가 &
2018 탈레스 데이터 위협 보고서 저자

## 암호화가 해결책

암호화 기술은 이동, 저장 및 사용 중인 데이터를 보호하는데 핵심입니다. 암호화는 규제 요건, 모범 관행, 개인정보 규정을 충족할 수 있도록 데이터를 보호해줍니다. 암호화는 기존의 데이터센터 내에서 데이터의 안전과 통제를 보장해줄 뿐만 아니라 기업의 디지털 트랜스포메이션을 추진해주는 기술들을 사용하는 유일한 툴입니다.

## 탈레스에 대하여

탈레스 이시큐리티는 정보가 생성, 공유 또는 저장되는 모든 곳에 신뢰성을 제공하는 선두적인 고급 데이터 보안 솔루션 및 서비스 전문업체입니다. 탈레스 이시큐리티는 온프레미스, 클라우드, 데이터센터, 빅데이터 환경 등 모든 환경에서 비즈니스의 민첩성에 영향을 주지 않고 비즈니스 및 정부 기관의 데이터를 보호하며 신뢰성을 제공합니다. 보안은 단지 위험을 절감하는 것에서 끝나지 않습니다. 디지털 화폐, 전자 ID, 헬스케어, 커넥티드 카, 사물인터넷, 심지어 가전 제품에 이르기까지, 보안은 이제 우리의 일상 생활에 깊숙이 자리잡은 디지털 이니셔티브들을 지원해줍니다. 탈레스는 암호화, 고급 키 관리, 토큰화, 사용자 접근 권한 통제 및 고신뢰성 솔루션을 통해, 조직들이 데이터, 식별 정보, 지적 재산을 보호 및 관리하고 규정 요건을 준수할 수 있도록 지원합니다. 탈레스에 대한 확신을 기반으로 전세계 보안 담당자들은 조직의 디지털 변혁을 가속화하고 있습니다. 탈레스 이시큐리티는 탈레스 그룹의 자사입니다.

보고서 전문을 확인하시려면 여기를 클릭하십시오.

후원

VENAFI

GEOBRIDGE

CSA cloud security alliance SM

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.co.kr