2023년 11월

기밀 컴퓨팅 ISV 구현 패키지

ISV가 인텔 기반 솔루션을 통해 고객의 비즈니스 문제를 해결하는 방법

기밀 컴퓨팅이란?

기밀 컴퓨팅이란?

기밀 컴퓨팅을 사용하면 민감한 데이터를 다른 소프트웨어, 공동 작업자 또는 클라우드 제공업체에 노출하지 않고도 인사이트를 추출하거나 AI 모델을 훈련할 수 있습니다.

이를 통해 기업이 이전에는 너무 민감하거나 규제로 인해 분석 및 기타 목적으로 활성화하기 어려웠던 데이터를 활용할 수 있는 폭넓은 가능성이 열립니다.

기밀 컴퓨팅 소프트웨어 세그먼트는 **가장 크고 가장 빠르게 성장하는 시장 세그먼트**가 될 것으로 예상되며, 그 뒤를 하드웨어와 서비스가 이을 것으로 전망됩니다.

불과 몇 년 만에 **기밀 컴퓨팅은 사용 중인 코드와 데이터를 엔드투엔드 방식으로 보호하는 강력하고 새로운 방법으로 광범위한 관심과 추진력을 얻었습니다.**

기밀 컴퓨팅의 필요성

데이터 보호 연속성에 존재하는 큰 격차를 해소합니다.

미사용 데이터	전송 중인 데이터	사용 중 데이터
스토리지 암호화	네트워크 암호화	기밀 컴퓨팅

Everest Group®

Everest Group에 따르면 이 "데이터 보안의 다음 프런티어는 ... 기하급수적인 성장을 맞이할 준비가 되어 있습니다."
2021년 19억 달러 규모였던 글로벌 시장은 클라우드 및 보안 프로젝트에 힘입어 2026년까지 40~95%의 연평균 성장률을 기록할 것으로 예상됩니다.

기밀 컴퓨팅
분야 & 사용 사례

분야

사용 사례

기밀 컴퓨팅
주요 AI 사용 사례

다자간 머신 러닝

민감한 고객 데이터의 기밀성과 개인정보를 손상하지 않으면서
머신 러닝의 힘을 활용하십시오.

비즈니스 요약

기밀 컴퓨팅을 통한 다자간 머신 러닝은 특히 다음 분야에서 유용할 수 있습니다.

의료

기밀 환자 정보를 노출하지 않고도 데이터의 힘을 활용하여 고급 연구를 수행할 수 있습니다.

금융 서비스

자금 세탁 및 테러 자금 조달과 싸우는 동시에 잠재적 사기 활동을 더 잘 예측할 수 있습니다.

고객 사례 연구

의료

규제 대상 데이터 기반 협업 컴퓨팅

BeeKeeperAI™ NOVARTIS

상황

Novartis Biome은 희귀 질환을 위한 진단 모델과 치료법을 개발합니다. 희귀 질환 정보는 여러 병원 및 연구기관에 드문드문 분산되어 있습니다.

과제

환자 정보는 비공개이며 엄격한 규제의 적용 대상입니다. 병원들은 오프프레미스로 데이터를 옮기거나 개인 기록을 BeeKeeperAI 또는 Novartis에 공개하기를 원하지 않습니다.

솔루션

각 병원의 온프레미스에 설치된 인텔® Software Guard Extensions(인텔® SGX) 기반 BeeKeeperAI 노드는 비공개 데이터를 분석하고 클라우드에 있는 마스터 모델 가중치를 업데이트합니다. Novartis나 BeeKeeperAI의 직원 모두 규제 대상 의료 기록을 보거나

BeeKeeperAI™

"[기밀 컴퓨팅 플랫폼]을 사용하면 알고리즘을 검증하는 주기를 절반으로 줄일 수 있습니다. 비용 또한 거의 절반으로 절감됩니다. 이러한 종류의 절감을 통해 일반화 가능한 알고리즘을 훨씬 더 빠르게 훈련하고 검증하고 시장에 출시할 수 있습니다. 또한, CCP의 기반이 되는 기술 및 프로세스가 성숙해짐에 따라 속도는 더욱 빨라지고 비용은 더욱 낮아질 것입니다."

MaryBeth Chalk, BeeKeeperAI, Inc., 공동 설립자 겸 최고상업책임자

백서

의료 AI 알고리즘의 개발 가속화

고객 사례 연구

높은 보안 수준의 키 보호

Fortanix®

상황

빠르게 확산되는 키와 인증서에는 강력한 보호와 중앙 집중식 관리가 필요합니다.
HSM 솔루션은 비용이 많이 들며, 클라우드 솔루션은 CSP 보안 및 규정 준수에 의존합니다.

과제

클라우드 호스트로부터 기술적으로 격리된 HSM과 같은 보안을 제공하는 확장 가능한 소프트웨어 기반 키 관리 시스템을 구축합니다.

솔루션

Fortanix는 인텔® SGX를 기반으로 자체 방어 KMS 소프트웨어를 구축하여 외부의 공격자 및 클라우드 제공업체로부터 키와 인증서를 보호하고 소유자가 자신의 기밀을 통제할 수 있도록 지원하고 있습니다.

Fortanix®

인텔® SGX의 사용에도 높은 성능을 유지하고 있습니다.
다중 인스턴스 구성을 구현하면 처리량이 크게 향상됩니다. 인텔® SGX의 사용은 이러한 성능 향상에 최소한의 영향을 미칩니다. 즉, 조직은 보안과 성능을 동시에 향상할 수 있습니다.

솔루션 스냅샷

기밀 AI 데이터 인텔 보안 솔루션 - Fortanix

PRC 고객 사례 연구

데이터 가치 마이닝

Chuanglin Technology

상황

엔터프라이즈 데이터 및 개인정보의 보안을 보장하는 방법은 데이터베이스 및 하드웨어 제조업체가 직면한 일반적인 문제입니다.

과제

기존의 데이터 암호화 기술은 하드디스크 스토리지 및 네트워크 전송만 암호화하며, 그 효과는 서버 제어 권한이 유출되지 않았다는 전제를 기반으로 합니다. 서버의 제어 권한을 가로채면 제3자가 사용 중인 데이터를 훔치거나 수정할 수 있습니다.

솔루션

Chuanglin Technology와 인텔은 인텔® SGX 메모리 암호화를 사용하여 그래프 데이터베이스 데이터 암호화 솔루션을 공동으로 출시했습니다. 이 솔루션은 Galaxybase의 궁극적인 성능을 보장하므로 메모리 안전형 그래프 데이터베이스 제품을 생성할 수 있습니다.

인텔® SGX 메모리 암호화 기술의 도움으로 Chuanglin Technology가 개발한 차세대 그래프 데이터베이스인 Galaxybase는 고객에게 더욱 안전한 고품질의 데이터 서비스를 제공하고, 데이터 상호 연결을 효율적으로 실현하고, 안정적인 방식으로 데이터 자산의 가치를 실현할 수 있도록 엔터프라이즈를 지원할 수 있게 되었습니다.

보도 자료

인텔이 기밀 컴퓨팅을 위해 제공하는 것

가장 포괄적인 보안 포트폴리오를 제공하는 인텔

인텔® Software Guard Extensions(인텔® SGX)

응용 프로그램 격리

인텔® Trust Domain Extension(인텔® TDX)

가상 머신 격리

인텔® Trust Authority

멀티 클라우드 및 하이브리드 클라우드에 대한 독립적인 신뢰 검증 서비스

소프트웨어 솔루션, 클라우드, OEM 및 시스템 통합자 생태계

인텔의 보안 우선 개발 및 수명 주기 지원

*일부 클라우드 제공업체를 통해 제공되는 인텔® TDX

Intel Trusted Execution 환경

응용 프로그램 수준 격리: 인텔® SGX

장점
- 클라우드 제공업체 및 기타 테넌트와의 분리
- 더 작은 신뢰 경계 및 잠재적 공격 표면
- 코드 검사 및 모니터링에 더 적합
- VM, 클라우드 네이티브 컨테이너 및 베어 메탈에 배포 가능

고려 사항
- 앱에는 특정 개발이나 조정이 필요할 수 있음
- 엔클레이브 외부에서 자주 호출하면 성능에 영향을 미칠 수 있음

VM 수준 격리: 인텔® TDX

장점
- 클라우드 제공업체 및 기타 테넌트와의 분리
- 기존 응용 프로그램에 대한 포팅 노력 최소화
- 전사적 배포 요구 사항에 더 적합
- 간단한 인스턴스 구성 설정이 가능

고려 사항
- 더 커진 신뢰 경계(게스트 OS, 모든 앱, VM 관리자)
- 업데이트된 게스트 OS 및 하이퍼바이저로 재검증 가능성
- 덜 세분화된 증명

인텔® Trust Authority

프라이빗 클라우드 보안으로 제로 트러스트를 실현하고 퍼블릭 클라우드 유연성 확보

인텔® Trust Authority는 제로 트러스트 원칙에 따라 기밀 컴퓨팅에 향상된 보안과 보증을 제공하는 새로운 소프트웨어 및 서비스 포트폴리오입니다.
1세대 인텔® Trust Authority는 (인텔® SGX) 및 (인텔® TDX)를 기반으로 하는 신뢰할 수 있는 실행 환경(TEE)을 입증하는 독립 증명 서비스를 제공합니다.

자체 증명 서비스를 구축하는 데 드는 비용과
복잡성 없이 제로 트러스트의 원칙을 구현합니다.

독립적 확장 가능 손쉬운 배포

자세한 정보

기밀 컴퓨팅 지원 패키지

제품 요약 | Noname 사례 연구 | Thales 사례 연구 | ZScaler 사례 연구 | 관련 비디오

인텔® Trust Authority
작동 방법

인텔® Trust Authority 시작하기

1

- 워크로드용 인텔® SGX 또는 가상 머신(VM)용 인텔® TDX를 기반으로 한 기밀 컴퓨팅 환경(TEE) 인스턴스를 설정하거나 클라우드 인프라 제공업체에 요청합니다.

2

- 기밀 컴퓨팅 환경에서 실행할 수 있도록 워크로드를 식별하고 활성화합니다.
- 인텔® SGX(Gramine 또는 다른 클라이언트 라이브러리에서 지원)의 응용 프로그램 수준 혹은 인텔® TDX의 VM 수준에서 수행할 수 있습니다.

3

- 구독하여 인텔® Trust Authority 증명 키를 받습니다.
- SaaS와 직접 통신하여 TEE를 검증할 수 있도록 워크로드(인텔® SGX) 또는 VM(인텔® TDX)의 클라이언트 라이브러리에 키를 삽입합니다.

인텔® Trust Authority에 등록하려면 intel.com/trustauthority를 방문하거나 trustauthority@intel.com에 문의하십시오.

인텔® Trust Authority 보안 솔루션에 대한 자세한 정보

기밀 컴퓨팅

인텔® SGX용 소프트웨어 및 솔루션 생태계

상업적으로 지원되는 솔루션

직접 구축

상용 솔루션 공급업체

anjuna
cosmian
CYBERNETICA
decentriq
EDGELESS SYSTEMS
Fortanix
Mithril Security
Opaque
enclaive
SCONTAIN
HUB SECURITY
secretarium

즉시 배포 가능한 선별된 컨테이너(2023년 1분기까지)*

PyTorch
redis
scikit learn
Spark
TensorFlow

개발자 도구

GRAMINE
SCONE
Occlum
Mystikos
Teaclave
Open Enclave SDK
intel
Intel SGX SDK

시스템 통합자

accenture
KPMG
Capgemini
IBM
Atos
leidos
avanade

하이퍼바이저(SGX)

KVM
5.13 이상
vmware
vSphere 8

* Azure Marketplace에서 사용 가능

인텔® TDX 가용성

인텔® TDX는 3가지 주요 클라우드 제공업체를 통해 4세대 인텔® 제온® 스케일러블 인스턴스에서 공개 미리 보기로 제공됩니다.

아래 로고를 클릭하여 각 클라우드 제공업체의 오퍼링을 자세히 알아보십시오.

Microsoft Azure Alibaba Cloud Google Cloud

IBM Cloud
*공개 미리 보기 추후 공고

인텔® TDX는 다음 게스트 OS 공급업체에서 지원합니다.

Red Hat SUSE Canonical Ubuntu

*인텔® TDX는 2024년부터 5세대 인텔® 제온® 스케일러블 프로세서에서 일반적으로 이용할 수

시작 방법

인텔® Software Guard Extensions (인텔® SGX)

추가 정보 시작하기

클라우드 서비스 제공 업체

자세한 정보를 보려면 로고를 클릭하십시오.

Azure CORE OVHcloud phoenixNAP GLOBAL IT SERVICES swisscom IBM Cloud CloudSigma

OEM

자세한 정보를 보려면 로고를 클릭하십시오.

Hewlett Packard Enterprise SUPERMICRO

교육 및 문서

교육 비디오 기술 라이브러리 솔루션 요약

인텔® Trust Domain Extensions (인텔® TDX)

추가 정보

문서

개발자를 위한 트러스트 도메인 보안 지침

시작하기

인텔® Trust Domain Extension(인텔® TDX) 모듈 다운로드

인텔® Trust Domain Extension(인텔® TDX) 로더

경쟁 제품과의 비교

	인텔® SGX	인텔® TDX	AMD SEV-SNP	AWS Nitro Enclaves	NVIDIA H100 GPU 기반 기밀 컴퓨팅
클라우드 인프라 제공업체의 하드웨어/펌웨어, 하이퍼바이저 및 클라우드 관리 스택은 신뢰 범위에서 제외됨	●	●	●		●
멀티 소싱을 용이하게 하기 위해 여러 클라우드 제공업체를 통해 사용 가능	●	●[1]	●		●
포팅, 재설계 또는 재패키징을 하지 않거나 적게 하고도 레거시 응용 프로그램을 수용하도록 설계됨		●	●		◎[2]
하드웨어 진위 여부 및 올바른 TEE 실행 여부 증명	●	●	●	●	●
TEE에 로드된 소프트웨어 이미지의 무결성 증명	●	◎[3]	◎[3]	●	
지정된 응용 프로그램 코드만 기밀 데이터에 액세스할 수 있고, VM 관리자, 게스트 OS, 기타 앱 및 클라우드 스택은 액세스에서 제외됨	●				
가상화 없이 "베어 메탈" 서버에 배포 가능	●				●
추가적인 Rowhammer 보호를 위한 하드웨어 기반, 암호화 메모리 무결성 옵션	●				
코드명이 Project Amber인 인텔의 독립 신뢰 서비스와 호환 가능	●	●			
2023년 3월 기준 경쟁력 데이터 출처			링크, 링크	링크, 링크, 링크	링크

[1] 인텔® TDX 인스턴스는 2023년 일부 클라우드 제공업체에서 온라인으로 제공될 예정이며, 가용 시기는 다를 수 있습니다.
[2] GPU에서 실행되는 레거시 코드의 경우 변경 사항이 없거나 적습니다. CPU를 사용하는 워크로드의 일부에는 CPU 기반 TEE와 PCIe 통신을 보호하는 수단을 통합해야 합니다.
[3] 가용 하드웨어 기술에 내재되는 기능은 아니지만, 클라우드 또는 증명 서비스 제공업체가 제공하는 부가 가치 기능으로 실현 가능합니다.

기밀 컴퓨팅을 위해 인텔을 선택해야 하는 이유는?

기밀 컴퓨팅을 위해 인텔을 선택해야 하는 이유는?

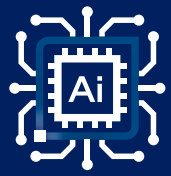
다양한 보안 요구 사항을 충족하는 기술 옵션

인텔만이 앱 격리(인텔® SGX)와 VM 격리(인텔® TDX)를 모두 제공하므로 고객은 다양한 수준의 보안을 위해 솔루션을 정밀하게 조정할 수 있습니다.

광범위한 솔루션 생태계

인텔은 수십 개의 ISV 및 클라우드 제공업체와 협력하여 기밀 AI, 분석, 블록체인, 데이터베이스 등을 포함한 호스팅 서비스 및 소프트웨어 솔루션을 제공하고 있습니다.

인텔 전문가 및 솔루션 파트너에 대한 액세스



인텔 전문가는 고객의 솔루션 아키텍처, 파트너 매칭, POC 리소스 및 배포 문제 해결을 지원할 준비가 되어 있습니다.

자세한 정보는 PSAM에 문의하십시오.

다음 단계

교육

기밀 컴퓨팅의 가치를 이해하고 많은 최종 사용자 앱이 환경의 안정성을 확인하고 다자간 계산을 활성화하는 데 기밀 컴퓨팅이 어떻게 필요한지 이해합니다.

관심 사로잡기

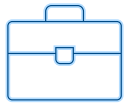
인텔 PSAM에 연결하여 생태계의 인텔 기밀 컴퓨팅 기술 포트폴리오에 관해 자세히 알아보십시오.

인텔® 파트너 얼라이언스의 지원 방법

인텔® 파트너 얼라이언스 시작하기

인텔® 파트너 얼라이언스 멤버십은 인텔의 글로벌 마켓플레이스 입점, 고급 교육 수강, 프로모션 지원을 비롯하여 독점적 비즈니스 구축 기회를 제공하며, 이 모든 것이 귀사의 필요에 맞춤화됩니다.

교육 및 역량

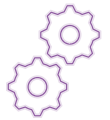


인텔® 파트너 유니버시티에 입학하면 고급 기술에 관한 전문 교육, 역량 프로그램 및 학습에 대한 보상이 제공됩니다.

마케팅 리소스

인텔 솔루션 마켓플레이스 및 인텔 마케팅 스튜디오에 입점하면 귀사의 제품 및 서비스에 대한 수요를 더 많이 창출하는 데 도움이 됩니다.

가치 있는 보상



적격 활동으로 포인트를 적립하고, 멤버십 등급을 높이고, 비즈니스 구축에 도움이 되는 추가 리소스에 액세스해 보십시오.

아직 회원이 아니라면
지금 가입하십시오

멤버십 혜택

포인트 적립

인텔® 파트너 얼라이언스 내에서 가장 인기 있고 차별화된 혜택 중 하나는 인텔과의 비즈니스 성과, 그리고 우선순위가 높은 활동에 대한 참여를 인정하기 위해 인텔이 파트너에게 지급하는 포인트입니다.

인텔® 파트너 얼라이언스 내에는 1,000가지가 넘는 포인트 적립 방법과 100가지가 넘는 포인트 사용 기회가 있습니다.

Cloud Insider 커뮤니티

인텔® 클라우드 인사이더 커뮤니티는 계속 새로워지는 세계 최고 수준의 클라우드 콘텐츠와 도구를 제공합니다. 회원에게는 동료 및 생태계와 연결하여 혁신적인 퍼블릭 클라우드 솔루션을 시장에 출시할 수 있는 기회가 주어집니다.

자세한 내용

업계 인사이트

Gold 및 Titanium 회원은 성장을 촉진하는 데 도움이 될 수 있도록 특별히 선별된 분기별 업계 인사이트에 액세스할 수 있습니다.

자세한 내용

재정적 인센티브

회원은 강력한 마케팅 개발 기금 및 인센티브 프로그램을 활용하여 제품 마케팅의 성공을 가속할 수 있습니다.

인텔® 파트너 얼라이언스 액셀러레이터 이니셔티브 및 추가 재정적 인센티브에 관해 알아보려면 PSAM에 문의하십시오.

intel partner alliance

고객 지원에 액세스하는 방법

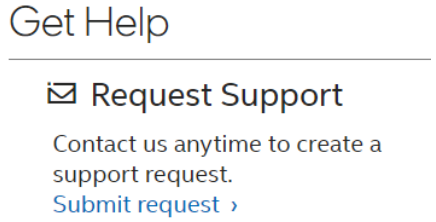
Intel Virtual Assistant

각 파트너 얼라이언스 웹 페이지에서 오른쪽 하단에 있는 이 채팅 봇은 대부분 질문에 셀프 도움말 또는 빠른 실시간 지원 담당자 연결을 제공합니다.

'블레이드' 도움말

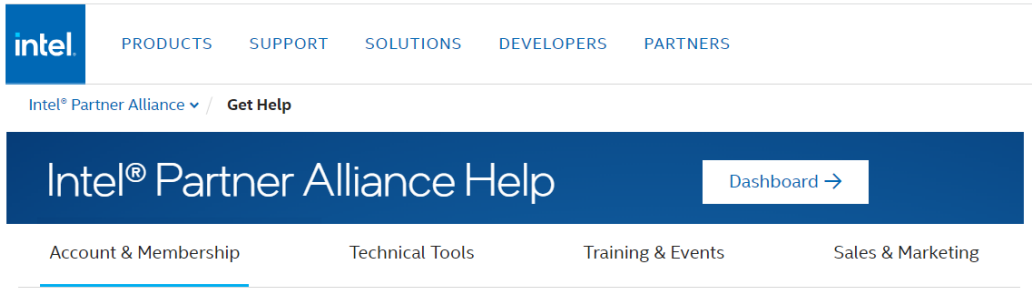
온라인 지원 요청을 제출하십시오.

파트너 얼라이언스 웹 사이트 내 대부분의 페이지 꼬릿말에 이 링크가 표시되어 있습니다.



파트너 얼라이언스 '도움말' 페이지

도움말 페이지는 파트너 얼라이언스 회원이 사용할 수 있는 대부분의 도구 및 혜택에 대한 자세한 자가 지원 가이드를 제공합니다.



리소스

Cloud TV

인텔® Cloud TV에서 성공을 촉진하기 위한 클라우드 컴퓨팅 뉴스, 동향 및 전략을 살펴볼 수 있습니다.

클라우드의 Sapphire Rapids

클라우드 자산을 보호하는 자세한 방법

클라우드에서의 보안

클라우드의 보안 과제

클라우드 솔루션 설계자 인증

CSA 커리큘럼을 이수하면 클라우드 인스턴스 세부 정보, 주제 및 솔루션에 대해 전문가 수준의 지식을 갖추게 됩니다.

이 커리큘럼은 클라우드에서 솔루션을 구현한 경험이 최소 2년 이상인 클라우드 솔루션 설계자에게 최적화되어 있습니다.

얻을 수 있는 이점

클라우드 기술 및 솔루션 아키텍처와 관련된 지식과 기술을 향상하여 클라우드 솔루션의 설계 및 구현을 보완합니다.
온라인용으로 설계된 대화형 과정과 수업을 통해 제공되는 최신 업계 동향에 관한 이해를 높입니다.
이를 통해 학습자는 쉽게 자신의 속도에 맞춰 발전하고 업무 및 개인 시간의 간섭을 최소화할 수 있습니다.
클라우드 기반 CI/CD 파이프라인을 통한 컨테이너 오케스트레이션, AI 워크로드 및 인스턴스 조정에서 다양한 클라우드 워크로드 전반의 고급 클라우드 응용 프로그램에 관한 고급 지식을 습득합니다.
주최/감독 시험을 기반으로 업계에서 인정받는 인증과 자격 증명을 얻습니다.

지금 자기 주도형 온라인 인증 교육을 시작하십시오.

기밀 컴퓨팅
정보 및 리소스

30-3-30

[기밀 컴퓨팅 30-3-30]

비디오

[기밀 컴퓨팅 개요]

[보안은 어려운 과제입니다]

연구 논문

[신흥 AI 워크플로 내에서 데이터 및 모델 보호하기]

기술 문서

[기밀 컴퓨팅의 현황]

[클라우드 보안 소개]

블로그

[성능 및 사이버 보안의 새로운 패러다임]

[보안은 인텔에서 시작됩니다]

기밀 컴퓨팅
DevOps 및 클라우드 설계자를 위한 리소스

기술 문서

기밀 컴퓨팅을 통한 가속화된 AI 추론

인텔® Security Engines를 통해 혁신을 가속하고 데이터 보호를 강화하십시오.

백서

새로운 사항 클라우드 보안 위협을 극복하는 방법

새로운 사항 기밀 컴퓨팅으로 소버린 랜딩 존 지원

뉴스레터

인텔 개발자 존 뉴스레터

커뮤니티

인텔 커뮤니티

보안 커뮤니티 파트너

비디오

인텔 보안 가속기 비디오

추가 리소스

성능 인덱스

4세대 인텔® 제온® 스케일러블 프로세서

웨비나 녹화본

클라우드 솔루션 아키텍트(CSA) 기술 강연: 4세대 인텔® 제온® 스케일러블 프로세서로 중요 워크로드 가속하기

라이브 웨비나

클라우드 솔루션 아키텍트(CSA) 기술 강연: 4세대 인텔® 제온® 스케일러블 프로세서를 통한 TCO 절감 및 효율성 향상

추가 교육

역량 및 인증

기밀 컴퓨팅
교육 링크

보안 교육 링크

과정/교육

주제 - 대상
사이버 보안 복원력을 높이는 3가지 핵심 기술 DevOps, 클라우드 설계자 - 기밀 컴퓨팅
IOT 솔루션을 위한 엔드 투 엔드 보안 DevOps
에지 투 클라우드 보안 DevOps, 클라우드 설계자
가상 프라이빗 클라우드, 클라우드 네트워킹, 클라우드 보안 DevOps
인텔® 제품 및 솔루션의 보안 가치 ALL
클라우드에서의 애플리케이션 보안 DevOps
클라우드 컴퓨팅의 보안 DevOps, Cloud Architects

주제 - 대상
가상 프라이빗 클라우드, 클라우드 네트워킹, 클라우드 보안 DevOps, 클라우드 설계자
비즈니스 보안에 관한 대화 클라우드 설계자, 최고 경영진
인텔 아키텍처 암호화 프라이머 DevOps
인텔® 제품 및 솔루션의 보안 가치 DevOps, 클라우드 설계자

보안 교육 링크

온라인 자습서

주제 - 대상
인텔® Hardware Shield 보안 기능을 활성화하는 방법 DevOps – 엔드 포인트 보안


intel