제품 요약

보안 가속
인텔® 제온® 스케일러블 프로세서

인텔® Security Engines를 통해 혁신을 가속하고 데이터 보호 강화

인텔® Security Engines와 5세대 인텔® 제온® 스케일러블 프로세서로 성능을 유지하면서 데이터 기밀성 및 코드 무결성을 유지합니다

인텔® 제온® 스케일러블 플랫폼 — 컨피덴셜 컴퓨팅으로 데이터를 실제로 활용하면서 비공개로 보호할 수 있습니다

지금은 데이터를 저장 및 전송 중인 동안 기본적으로 암호화합니다. 하지만 기업은 데이터가 프로세서와 메모리에서 실제로 사용 중일 때 데이터를 보호해야 하는 문제에 직면합니다. 이 시점에 개인 식별 정보, 의료 기록 및 금융 거래 같은 민감한 데이터가 잠재적인 악용이나 노출 사고나 법규 준수 위반에 취약해집니다.

데이터가 점점 중요해지는 세상에서, 비즈니스는 데이터를 무단 액세스로부터 보호해야 합니다. 인텔® Security Engines가 탑재된 인텔® 제온® 스케일러블 프로세서는 하드웨어 기반 컨피덴셜 컴퓨팅 솔루션을 제공하므로, 비즈니스는 데이터를 비공개로 유지하면서 인사이트를 얻거나 AI 모델을 배포하고 데이터의 힘을 활용할 수 있습니다.

5세대 인텔® 제온® 프로세서를 사용하면 비즈니스는 프로세서 안에 안전한 보안 엔클레이브를 만들고 거기에서 민감한 데이터를 다른 소프트웨어, 공동 작업자 또는 클라우드 제공업체에 노출시키지 않고 처리 및 분석할 수 있습니다. 따라서 과거에는 너무 민감하거나 규제되어 분석할 수 없었던 데이터를 사용할 수 있는 새로운 가능성이 열립니다. 5세대 인텔® 제온® 스케일러블 프로세서는 사용 중인 데이터를 보호하여 조직이 개인정보보호 및 법규 준수 의무를 다하는 데에도 도움이 될 수 있습니다.

이런 보안 엔클레이브를 사용하면 데이터가 실제로 사용 중인 동안 무단으로 액세스되지 않도록 보호됩니다. 인텔® Software Guard Extensions(인텔® SGX)와 인텔® Trust Domain Extensions(인텔® TDX)를 모두 탑재한 인텔® 제온® 스케일러블 프로세서를 사용하는 고객은 비즈니스 및 규제 요구 사항을 가장 잘 충족하는 컨피덴셜 컴퓨팅 기술을 선택할 수 있습니다.

인텔® SGX와 인텔® TDX로 컨피덴셜 컴퓨팅 수용

인텔® SGX를 사용한 컨피덴셜 컴퓨팅은 애플리케이션 또는 기능 수준 격리를 지원합니다. 클라우드, 에지 또는 온프레미스 등 어디에서나 민감한 연산과 데이터가 클라우드 서비스 제공자, 권한 없는 관리자, OS 및 기타 권한 있는 애플리케이션으로부터 더 안전하게 비공개로 유지됩니다.

고객 성공 사례: 인텔® 제온® 스케일러블 프로세서를 사용한 보안으로 혁신 주도

인텔® 제온® 스케일러블 프로세서는 BeeKeeperAI가 의료용 머신러닝 알고리즘을 개발하는 데 도움이 되는 한편, 민감한 데이터도 안전하게 보호합니다. 데이터 관리자는 인텔® SGX를 사용하여 소비하는 AI 애플리케이션의 무결성을 확인할 수 있습니다.

자세히 알아보기 ›

Zscaler의 클라우드 네이티브 Zero Trust Exchange 플랫폼은 사용자, 장치 및 애플리케이션을 어떤 위치에서든 안전하게 연결합니다. Zscaler는 자사의 Zero Trust Exchange와 앱 커넥터를 인텔® TDX TEE에서 격리하고 인텔® Trust Authority를 사용하여 여러 클라우드 인프라에 걸쳐 그 신뢰성과 무결성을 확인합니다.

사례 읽기 ›

풍부한 변화 기회

- AI를 사용한 분석 및 서비스
- 클라우드 경제와 규모
- 분산 및 에지 애플리케이션
- 새로운 데이터 소스로 지원되는 서비스 혁신
- 개인정보보호 유지 기술
- 블록체인 기반 서비스
- 데이터 중심 다자 협업

인텔® SGX는 가장 많이 연구되고 업데이트되는 데이터 센터용 신뢰 실행 환경(TEE)이며, 시스템 안에서 가장 작은 공격 표면을 제공합니다.[1] 인텔® 제온® 스케일러블 프로세서의 이 기능은 여러 클라우드와 에지에서 컨피덴셜 컴퓨팅 솔루션의 구성 요소로 사용됩니다.

인텔® SGX는 특별한 애플리케이션 격리 기술을 통해 사용 중인 데이터를 보호하는 데 도움이 되는 하드웨어 기반 보안 솔루션을 제공합니다. 개발자는 선택된 코드와 데이터를 조사 또는 수정하지 못하도록 보호함으로써 민감한 데이터 작업을 엔클레이브 안에서 실행하여 애플리케이션 보안을 강화하고 데이터 비밀을 보호할 수 있습니다.

또한 인텔® SGX의 인증 기능을 사용하면 엔클레이브 안에서 실행 중인 소프트웨어가 모든 당사자가 예상했고 이전에 합의했던 소프트웨어와 정확하게 일치함을 더욱 확신할 수 있습니다.

인텔® SGX는 애플리케이션 및 기능 격리에 사용되는 한편, 인텔® TDX는 가상머신(VM) 수준에서 격리와 비밀유지 기능을 제공합니다. 이 도구는 게스트 OS와 VM 애플리케이션을 플랫폼의 클라우드 호스트 및 하이퍼바이저와 기타 VM으로부터 격리합니다. 인텔® TDX의 신뢰 범위는 인텔® SGX의 애플리케이션 수준 격리보다 크지만, 인텔® TDX는 컨피덴셜 VM을 애플리케이션 엔클레이브보다 더 쉽게 배포 및 관리할 수 있도록 설계되었습니다. 인텔® TDX는 기존 애플리케이션을 TEE로 이동하는 더 간단한 마이그레이션 경로를 제시하기도 합니다. 고객은 TDX가 있는 5세대 인텔® 제온® 스케일러블 플랫폼에서 TDX가 없는 4세대 인텔® 제온® 스케일러블 플랫폼보다 최대 11% 더 높은 가상 머신 성능(정수, 부동소수점 및 BERT-large 기준)을 얻을 수 있습니다.[2]

데이터 분석의 속도를 높이면서 법규 준수 개선

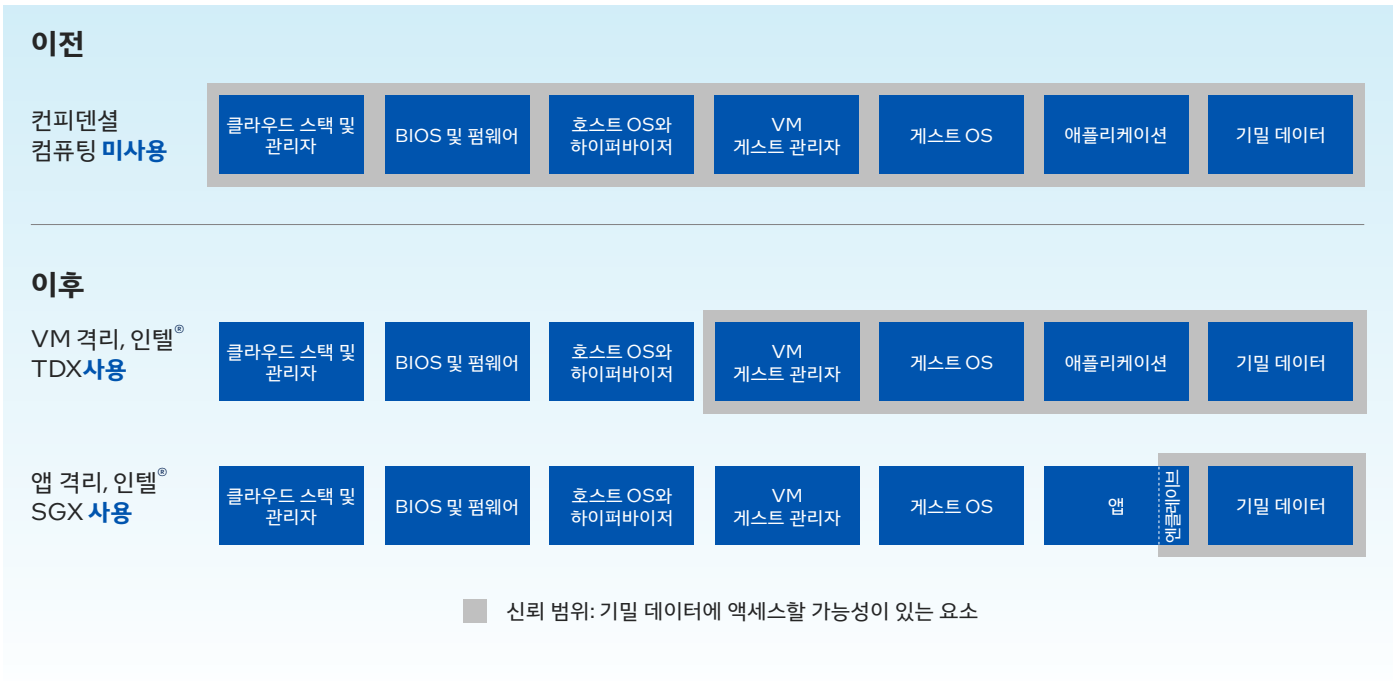
비즈니스에 가치가 있는 데이터에는 일반적으로 엄격한 개인정보보호 법규가 적용됩니다. 이런 법규를 위반하면 많은 벌금을 물거나 다른 처벌을 받을 수 있기 때문에 조직이 민감한 데이터를 완전히 활용하려면 위험이 따릅니다. 개인 식별 정보 사용을 대체할 차선책을 선택할 수도 있지만, 종종 분석 프로세스의 속도가 크게 저하되고 정확성도 떨어질 수 있습니다. 비즈니스는 5세대 인텔® 제온® 스케일러블 프로세서와 인텔의 컨피덴셜 컴퓨팅 포트폴리오로 데이터와 애플리케이션의 기밀성을 유지하는 데 도움이 되는 암호화된 엔클레이브를 만들어 법규 준수와 데이터 가용성을 모두 개선할 수 있습니다.

"GDPR에 의거한 데이터 유출 비용은 총 연매출의 4%에 이를 수 있으므로, 데이터 관리자는 사용 중인 데이터를 포함한 잠재적인 공격 표면을 공격으로부터 보호해야 합니다."

- 컨피덴셜 컴퓨팅 컨소시엄, 2022년 11월[3]

민감한 데이터의 공유를 방해하는 요인 제거

엔티티 간에 데이터를 공유하면 신경망 학습 같은 비즈니스 프로세스가 훨씬 더 정확하고 빨라질 수 있습니다. 5세대 인텔® 제온® 스케일러블 프로세서를 사용하면 연합 학습 같은 신뢰할 수 있는 다자 컴퓨팅 모델을 통해 비밀 데이터를 공유할 수 있습니다. 인텔 컨피덴셜 컴퓨팅 기술이 적용된 5세대 제온® 스케일러블 프로세서를 사용하면 여러 당사자가 민감한 데이터를 풀링하여 비공개 데이터를 권한 없는 사용자에게 노출시키지 않고 공통 분석의 이점을 함께 누릴 수 있습니다.



인텔® Crypto Acceleration과 인텔® QuickAssist Technology(인텔® QAT)를 활용하여 보안-보호 성능 강화

지금의 데이터 센터는 데이터를 보호하기 위해 노력하면서 암호화를 기존의 경계 방어 이외에 네트워킹, 스토리지 및 데이터 압축 같은 광범위한 프로세스에도 사용합니다. 암호화가 증가함에 따라 CPU에서 수행해야 하는 암호화 사이클의 수도 폭증하고 있습니다. 그 결과 성능과 사용자 경험이 악화될 수 있습니다.

5세대 인텔® 제온® 스케일러블 프로세서에 내장된 첨단 암호화 가속 기술을 사용하면 더 많은 코어와 프로세서를 데이터 센터에 추가해야 할 필요 없이 암호화 보안 수준을 높이고, 성능을 높이고, 보다 원활한 사용자 경험이 가능할 수 있습니다.

성숙한 데이터 압축 및 암호화 가속기인 인텔® QAT는 5세대 인텔® 제온® 스케일러블 프로세서의 내장형 가속기에 통합되어 데이터를 즉시 압축/압축 해제하고 암호화하는 워크로드에 사용됩니다. 인텔® QAT는 컴퓨팅 집약적인 워크로드의 부하를 덜어 다른 워크로드에 사용 가능한 코어 용량을 확보하면서 비용과 압축 데이터 공간을 크게 줄이는 데 도움이 될 수 있습니다.[4] 고객은 QAT가 내장된 5세대 인텔® 제온® 플래티넘 8592+로 4세대 AMD EPYC 9554 OOB보다 코어당 최대 1.85배 더 높은 NGINX TLS 핸드셰이크 성능을 얻을 수 있습니다.[5]

인텔® Crypto Acceleration 명령어는 더 큰 키 크기, 더 강력한 알고리즘, 더 많은 데이터 유형 암호화 같은 더 강력한 암호화 프로토콜을 사용하고 UX에 미치는 영향을 최소화합니다. 사용자는 더 빠른 암호화 알고리즘을 이용하여 성능 개선, 더 나은 서비스 수준 계약(SLA) 지원, 암호화 처리에 일반적으로 사용되는 컴퓨팅 사이클 감소가 가능합니다.

암호화 가속은 알고리즘 수준에서 다음과 같은 세 가지의 주요 암호화 컴퓨팅 분야에서 성능을 높입니다.

공개 키 암호화: SSL(Secure Sockets Layer), 프론트엔드 웹 및 공개 키 인프라(PKI) 같은 용도에 사용.

대량 암호화: 보안 데이터 전송, 디스크 암호화 및 스트리밍 비디오 암호화 같은 용도에 사용.

해싱: 디지털 서명, 인증, 그리고 SHA-1(Secure Hash Algorithm 1)과 SSL에서 사용하는 SHA-2(Secure Hash Algorithm 2, SHA-256이라고도 함) 같은 무결성 확인 등의 용도에 사용.

Microsoft, SAP 및 Oracle 같은 회사의 여러 상용 소프트웨어 패키지는 인텔® Crypto Acceleration을 이용하도록 최적화되었습니다. 인텔은 인텔® Crypto Acceleration을 지원하도록 오픈 소스 소프트웨어(다양한 Linux 배포, NGINX, Java OpenJDK 런타임, OpenSSL 라이브러리)를 최적화하였습니다.

암호화 API 툴킷 같은 개발자 도구는 인텔® SGX 엔클레이브 안에서 암호화 작업을 더 안전하게 실행할 수 있습니다. 또한 인텔® Integrated Performance Primitives(인텔® IPP) 라이브러리는 사용 가능한 CPU 기능을 자동으로 이용하는 한편, OpenSSL용 인텔® QAT 엔진을 통해 네트워크 보안 소프트웨어 솔루션은 인텔® Crypto Acceleration을 투명하게 이용할 수 있습니다.

인텔® 제온® 프로세서에 내장된 암호화 가속 기술을 활용하면 기업에서 암호화 처리에 쓰는 컴퓨팅 사이클을 줄이고 UX를 개선할 수 있습니다.

Thales의 엔드투엔드 데이터 보호 지원

Thales와 인텔은 컨피덴셜 컴퓨팅이 널리 사용되도록 하고 CipherTrust 데이터 보안 플랫폼에서 사용하는 데이터를 보호하는 기능을 추가하기 위해 협력하고 있습니다. 인텔과 Thales는 함께 클라우드 및 온프레미스 환경을 모두 지원하는 광범위한 엔드투엔드 데이터 보호 솔루션을 제공하는 신뢰할 수 있고 조화를 이루는 에코시스템을 만들어 고객 민감 워크로드의 암호를 해독하기 전에 환경의 신뢰성을 인증합니다.

인텔® Trust Authority에서 제공하는 신뢰할 수 있는 인증을 사용하므로, Thales의 CipherTrust 데이터 보안 플랫폼의 민감한 워크로드가 인텔® TDX 또는 인텔® SGX TEE 밖에서 암호화되지 않습니다. Thales의 CipherTrust 데이터 보안 플랫폼은 FIPS 140-2 레벨 3를 준수합니다.

이 기술의 여러 업계 이용 사례가 있습니다. 예를 들어 의료 업계에서 환자 데이터세트를 사용한 머신러닝 모델 학습이 가능해지면 질병 진단과 의약품 개발이 용이해질 수 있습니다. 은행업에서는 여러 은행이 개인 정보 유출 없이 데이터를 공유할 수 있고, 그러면 자금 세탁이나 다른 불법 거래를 적발하는 데 도움이 됩니다.

클라우드와 데이터 센터에 대한 폭넓고 확장 가능한 신뢰

5세대 인텔® 제온® 스케일러블 프로세서에 탑재된 인텔® Security Engines는 비즈니스가 클라우드의 유연성과 확장성을 이용하면서 민감한 데이터를 노출시킬 위험을 줄이는 데 도움이 됩니다. 인텔® 제온® 스케일러블 프로세서를 사용한 컨피덴셜 컴퓨팅은 민감한 데이터를 클라우드 제공자의 소프트웨어, 관리자 및 기타 테넌트로부터 격리합니다. 데이터 소유자는 원격 인증을 사용해 각 테넌트의 엔클레이브가 진짜이고 최신 상태이고 예상한 소프트웨어만 실행하는지 확인할 수 있습니다.

지금 인텔® 제온® 스케일러블 프로세서를 선택하여 데이터로 더 많은 작업을 수행하세요

인텔® Security Engines가 내장된 인텔® 제온® 스케일러블 프로세서는 전세계의 클라우드 제공업체 및 시스템 제조업체를 통해 제공됩니다. 이 프로세서는 새로운 서비스를 개선하고, 트랜잭션의 가치를 높이고, 금융 범죄를 방지하고, R&D 주기를 단축하고, 민감하거나 가치 있거나 규제되는 데이터가 사용되는 애플리케이션의 발전을 촉진하기 위해 사용할 수 있습니다.

미래는 데이터를 가진 이들의 것이며, 인텔® Security Engines로 이런 미래를 앞당길 수 있습니다.

인텔® Security Engines의 도움으로 비즈니스에 가장 중요한 워크로드의 성능과 보안을 극대화할 수 있는 방법에 대해 자세히 알아보십시오.

컨피덴셜 컴퓨팅 ›

인텔® Security Engines ›

1. https://www.intel.co.kr/content/www/kr/ko/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html
2. intel.com/processorclaims: 5세대 인텔® 제온® 스케일러블 프로세서에서 [S1]을 참조하십시오. 결과는 다를 수 있습니다.
3. Confidential Computing: Hardware-Based Trusted Execution for Applications and Data(컨피덴셜 컴퓨팅: 하드웨어에 기반한 애플리케이션과 데이터의 신뢰할 수 있는 실행)," The Confidential Computing Consortium 2022년 11월, V1.3, https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf
4. https://www.intel.com/content/www/us/en/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html
5. intel.com/processorclaims: 5세대 인텔® 제온® 스케일러블 프로세서에서 [N202]를 참조하십시오. 결과는 다를 수 있습니다.