

▶ 둘러보기

Dell Trusted Workspace



어디서나 안전하게 업무 수행

오늘날의 클라우드 기반 환경에 맞게 구축된 하드웨어 및 소프트웨어 방어 체계를 제공합니다.

조직은 하이브리드 근무 방식 때문에 새로운 공격 벡터에 노출되고 있습니다. 공격자들이 점점 정교한 기술을 사용하는 오늘날, 효과적인 엔드포인트 보안을 위해 디바이스와 네트워크, 클라우드를 다층적으로 보호할 필요가 있습니다.

포괄적인 하드웨어 및 소프트웨어 보호 포트폴리오를 통해 공격 노출 지점을 축소하고 최신 위협보다 한발 앞서 나가십시오.

[포트폴리오에 대한 자세한 정보 →](#)



세계적 수준의 보안을
자랑하는 커머셜 AI PC¹ →



전체 시스템의 보안을
향상하는 소프트웨어 →

다중 방어 계층

추가 구축된 소프트웨어 보안 기능

전문적으로 선정된 파트너 생태계의 소프트웨어로 지능형 공격을 다층적으로 방어합니다. 보안 솔루션 구매를 통합하여 얻을 수 있는 이점과 효율성을 활용하십시오.

내장된 하드웨어 및 펌웨어 보안

세계적 수준의 보안을 자랑하는 AI PC를 통해 근원적인 공격을 탐지하고 방지합니다.¹ BIOS/펌웨어 및 하드웨어 수준에서의 심층 방어를 통해 사용 중인 디바이스를 보호합니다.

Dell은 PC 텔레메트리와 업계를 선도하는 소프트웨어를 통합하여 전체 시스템의 보안을 개선합니다.¹

기본 구축된 공급망 보안

처음 부팅하는 순간부터 보안이 유지되는 디바이스로 안심하고 작업하십시오. 안전한 PC 설계, 개발, 테스트를 통해 제품 취약성으로 인한 위험을 최소화합니다. 엄격한 공급망 관리로 제품 변조의 위험을 완화합니다.



위협의 발생
위치에 관계없이
위협 예방, 탐지
및 대응

**Dell SafeGuard
and Response**

Dell SafeData



진화하는
위협으로부터
보안 유지

Dell SafeBIOS

Dell SafeID

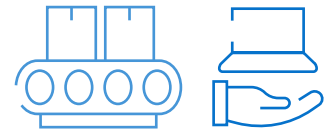


배송 시
변조되지 않는
신뢰할 수 있는
하드웨어

**Dell SafeSupply
Chain**

Dell Trusted Workspace 기본 구축 및 내장된 기능

세계적 수준의 보안 기능을 갖춘 커머셜 AI PC¹



처음 부팅하는 순간부터 보안 유지

엄격한 첨단 공급망 관리와 Dell 고유의 보안 구성 요소 검증과 같은 추가 기능 옵션을 통해 PC 무결성을 보장합니다. [자세한 정보](#) →

BIOS 무결성 유지

Dell 고유의 BIOS 검증 기능인 **SafeBIOS**를 통해 위협을 포착하고 차단합니다. 손상된 BIOS를 진단 및 복구하고 향후 위협에 대한 노출을 줄이는 통찰력을 확보할 수 있습니다. [자세한 정보](#) →

펌웨어 무결성 검증

인텔 프로세서에 탑재된 하드웨어 기반 보안 기능인 Dell의 독보적인 **펌웨어 검증** 기능은 높은 권한을 갖는 펌웨어에 대한 무단 액세스와 변조를 방지합니다. [자세한 정보](#) →

급박한 위협 감지

Dell에서 제공하는 조기 알림 기능인 **IoA(Indicator of Attack)**는 손상이 발생하기 전에 행동 기반 위협을 검사합니다. [자세한 정보](#) →

최종 사용자 자격 증명 보안

멀웨어로부터 사용자 자격 증명을 숨기는 전용 보안 칩인 Dell 고유의 **SafeID**로 사용자 액세스 권한을 확인합니다. [자세한 정보](#) →

알려진 취약점 포착

Dell 고유의 **CVE(Common Vulnerabilities and Exposures)** 탐지 기능은 공개적으로 보고된 BIOS 보안 결함을 모니터링하고 위험 완화 업데이트를 권장합니다. [자세한 정보](#) →



*Principled Technologies가 검증한 업계 선도적 위상**

PC 텔레메트리로 IT 보안 격차 완화

OS 아래 계층 통찰력으로 소프트웨어 솔루션 강화 Dell은 PC 텔레메트리와 업계를 선도하는 소프트웨어 공급업체를 독보적으로 통합하여 전체 시스템의 보안을 개선합니다.¹ [자세한 정보](#) →

Dell Trusted Device 둘러보기



[노트북](#) →



[데스크탑](#) →



[워크스테이션](#) →

*연구 결과는 인텔 기반 디바이스에만 사용할 수 있습니다.

Copyright © Dell Inc. All Rights Reserved.

DELLTechnologies

Dell Trusted Workspace 추가 구축된 보안

전체 시스템의 보안을 향상하는 소프트웨어



Dell SafeGuard and Response 로 지능화된 사이버 공격 방지

발생 위치에 관계없이 위협을 예방하고 탐지 및 대응하십시오. 인공 지능과 머신 러닝을 활용하여 사전 예방적으로 엔드포인트 공격을 탐지하고 차단하는 한편, 보안 전문가가 엔드포인트, 네트워크 및 클라우드 전반에 걸쳐 식별된 위협을 추적하고 문제를 해결할 수 있도록 지원합니다.

Partners

[CrowdStrike Falcon®](#) →

[Sophos | Secureworks® Taegis™ XDR](#) →

Dell SafeData로 디바이스 및 클라우드의 데이터 보호

사용자가 어디에서나 안전하게 협업할 수 있도록 지원합니다. Netskope는 데이터 중심의 클라우드 보안 및 액세스 방식을 통해 위치에 관계없이 데이터와 사용자를 보호하고, Absolute는 회사 방화벽 외부에서 IT 가시성, 보호 및 지속성을 제공합니다.

Partners

[Absolute](#)를 사용한 엔드포인트, 앱, 네트워크 자동 복구 →

[Netskope](#)를 사용한 Security Service Edge 솔루션 둘러보기 →

Dell Security Services 둘러보기

Dell 고객은 보안을 직접 관리할 수도 있고, 전문가가 대신 관리하도록 맡길 수도 있습니다. Dell의 완전 관리형 360° SecOps 솔루션은 IT 환경에서 보안 위협을 방지하고 대응 및 복구하도록 설계되었습니다.

[Managed Detection and Response Pro Plus에 대한 자세한 정보 →](#)



Dell Trusted Workspace 하드웨어 지원 보안

통합 보안

사이버 위협이 진화하면서 소프트웨어에만 의존하는 방어를 우회하고 있습니다.
하드웨어 지원 보호를 통해 엔드포인트의 공격 노출 지점을 줄여보십시오.

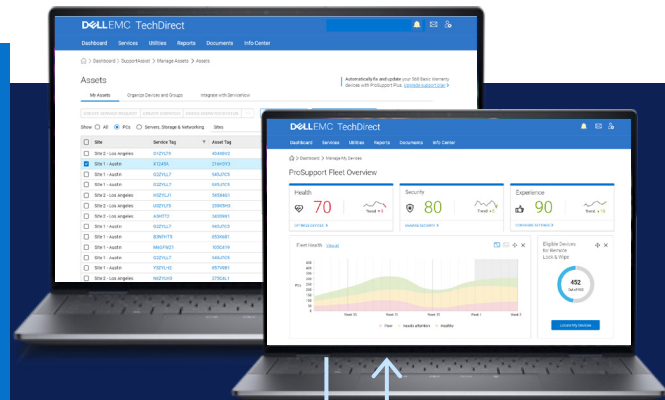
최신 위협을 방지하려면 하드웨어 방어와 소프트웨어 방어가 함께 작동해야 합니다. Dell은 이러한 부분에 도움을 드릴 수 있습니다. Dell은 업계를 선도하는 보안 파트너와 함께 손잡고 풍부한 디바이스 레벨 텔레메트리와 첨단 위협 탐지 기능을 결합하여 전체 시스템의 보안을 개선합니다.

- ✓ 공격 노출 지점 축소
- ✓ 공격 탐지 기능 향상

- ✓ 디바이스 신뢰성 유지
- ✓ 공급업체 통합

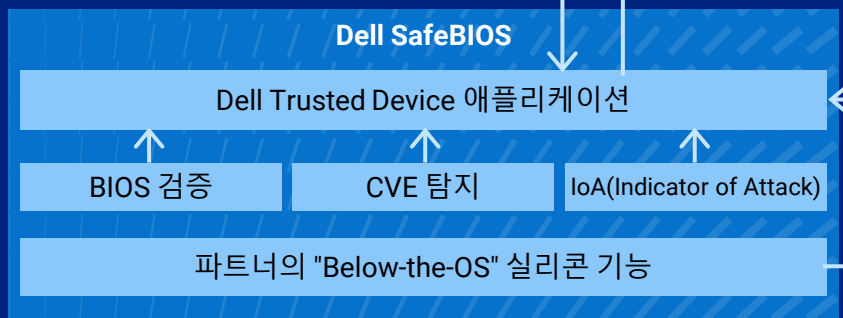
추가 구축된
소프트웨어 보안 기능

PC 텔레메트리와
업계를 선도하는
소프트웨어를
통합하여 전체
시스템의 보안을
개선^{1,2}

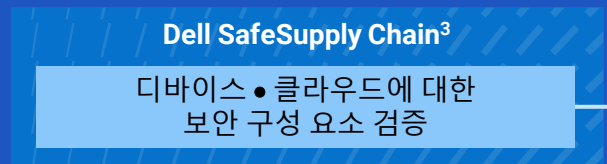


OS

내장된 하드웨어 및
펌웨어 보안 기능



기본 구축된
공급망 보안



Dell Trusted Workspace로 어디서나 안전하게 업무를 수행하십시오.



타사 솔루션과 연동하는
내장된 하드웨어 보안



추가 구축되는
소프트웨어 보안 기능

다중 방어 계층으로
공격 노출 지점을
줄이고 장기적인
사이버 회복탄력성을
개선합니다.

웹사이트

dell.com/endpoint-security

연락처

global.security.sales@dell.com

자세한 정보

[Endpoint Security 블로그 →](#)

대화에 참여

[LinkedIn /delltechnologies](#)

[X @delltech](#)

출처 및 법적 고지 사항

¹Dell 내부 분석 기준, 2024년 10월(인텔) 및 2025년 3월(AMD). 인텔 및 AMD 프로세서를 탑재한 PC가 해당됩니다. 모든 PC에서 모든 기능을 사용할 수 있는 것은 아닙니다. 일부 기능을 사용하려면 추가로 구매해야 합니다. Principled Technologies에서 검증한 인텔 기반 PC입니다. A comparison of security features, 2024년 4월. ²CrowdStrike Falcon Insight XDR 및 Absolute에 사용할 수 있는 통합 기능입니다. ³사용 가능 여부는 지역에 따라 다릅니다.