DELL Technologies

Trusted Device 분석

Dell이 세계 최고 수준의 보안을 자랑하는 커머셜 AI PC[1]인 이유 알아보기

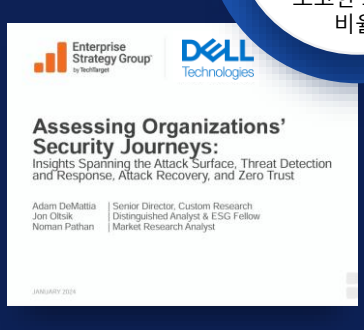
위협 환경 및 당면 과제

OS 아래 계층을 대상으로 한 공격 벡터로 새로운 위험 야기

엔드포인트 디바이스는 보안 침해가 주로 발생하는 게이트웨이입니다. 하이브리드 방식의 근무로 인해 공격 노출 지점이 확대됨에 따라 최근 디바이스 보안에 대한 우려가 커졌습니다. 공격자가 기존 EDR 소프트웨어만으로는 대부분 탐지할 수 없는 루트킷 및 기타 펌웨어 취약성뿐 아니라 공급망을 표적으로 삼는 사례가 증가하고 있습니다.

디바이스 기반 위협은 2020년 이후 1.5배 증가했습니다.[2]

69%
디바이스/BIOS 수준 공격을 1회 이상 보고한 조직의 비율[2]



새로운 PC 조달 시 주요 평가 기준:

- BIOS 이벤트 자동 탐지[3]
- 고위험 구성 처리[3]

최신 위협에 대처하려면 디바이스를 안전하게 구축하면서 공격 포착 및 차단이 가능한 보안 기능을 갖추어야 합니다.

솔루션

근본적인 공격의 예방, 탐지, 대응 및 복구 세계 최고 수준의 보안 기능을 갖춘 PC로 대응[1]

시스템 전체의 보안은 개별 PC의 보안에 좌우됩니다. 그렇다면 어떤 요소가 디바이스의 신뢰성과 보안을 보장할까요? 바로 가시성과 실행 가능성입니다. 더 많은 데이터에 액세스할 수 있으면 합리적인 의사 결정이 가능해져 교묘한 형태의 신종 위협도 포착할 수 있습니다. 자동화를 통해 잠재적 문제를 더욱 빠르게 해결할 수 있습니다.

Dell 커머셜 PC(인텔 및 AMD)의 하드웨어 및 펌웨어 방어 기능은 가시성과 실행 가능성을 확보하도록 설계되었습니다.

Dell Trusted Devices 분석

이점

- 엄격한 공급망 관리로 첫 부팅부터 안전성 보장
- 펌웨어 수준의 정보를 구체적으로 표시하여 BIOS의 무결성 유지
- 자격 증명 도용 멀웨어로부터 사용자 ID 보호
- 'OS 아래 계층' 텔레메트리로 OS 수준 데이터를 보강함으로써 탐지, 대응 및 문제 해결 속도 향상

PC 텔레메트리로 보안 개선

OS 아래 통찰력으로 IT 보안 격차를 좁히고 소프트웨어 솔루션을 강화할 수 있습니다. Dell은 PC 텔레메트리와 업계를 선도하는 소프트웨어 공급업체를 통합하여 전체 시스템의 보안을 개선합니다.[1]
자세한 정보 →

BIOS 무결성 유지

Dell의 독보적인 BIOS 검증 기능을 통해 위협을 포착하고 차단합니다. BIOS 이미지 캡처를 통해 손상된 BIOS를 평가하고 복구한 후 향후 위협에 노출될 가능성을 줄이는 인사이트를 얻을 수 있습니다.[1]
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.[1]

급박한 위협 감지

Dell의 독보적인 조기 경보 기능인 IOA(Indicators of Attack)를 통해 동작 기반 위협이 실제 손상을 일으키기 전에 파악할 수 있습니다.[1]
자세한 정보 →

알려진 취약점 포착

Dell의 독보적인 CVE(Common Vulnerabilities and Exposures) 탐지 기능은 공개적으로 보고된 BIOS 보안 결함을 모니터링하고 위험 완화 업데이트를 권장합니다.[1]
자세한 정보 →

최종 사용자 자격 증명 보안

멀웨어로부터 사용자 자격 증명을 숨기는 전용 보안 칩인 Dell의 독보적인 SafeID로 사용자 액세스 권한을 확인합니다.[1]
자세한 정보 →

PC 수명 주기 전반에서 보안 유지

엄격한 첨단 공급망 관리와 Dell의 독보적인 SCV(Secured Component Verification) 등 추가 기능 옵션을 통해 제품 수령부터 수명 주기 전반에 걸쳐 PC 무결성을 보장합니다.[1]
자세한 정보 →

업계 선도적 위상

Dell은 PC 제조업계에서 독보적으로 BIOS 수준의 가시성을 제공합니다.[1]

최신 위협에 대한 디바이스 신뢰를 유지하기 위해 무엇이 필요한지 알아보십시오.[4]

자세한 정보 →

A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

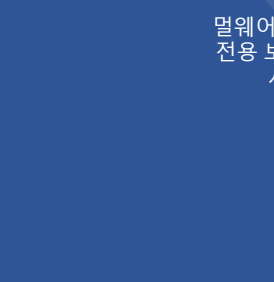
Approach

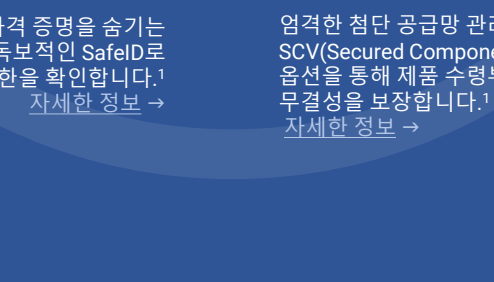
Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

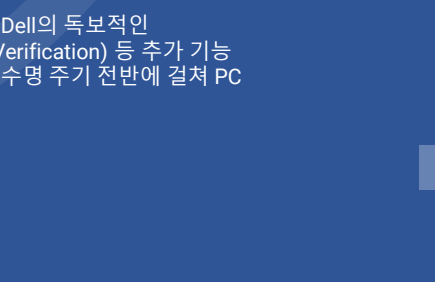
- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original

Dell Trusted Device 둘러보기


노트북 →


데스크탑 →


워크스테이션 →

Dell Trusted Workspace로 어디서나 안전하게 업무 처리

타사 솔루션과 연동하는 내장된 하드웨어 보안

추가 구축되는 소프트웨어 보안 기능

웹사이트
dell.com/endpoint-security

연락처
global.security.sales@dell.com

자세한 정보
Endpoint Security 블로그 →

대화에 참여
delltechnologies @delltech

출처 및 법적 고지 사항

[1]Dell 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 Technologies의 검증을 받았습니다. A comparison of security features, 2024년 4월.

[2]출처: Futurum Group, Endpoint Security Trends, 2023년.

[3]출처: TechTarget 부서인 Enterprise Strategy Group이 Dell Technologies 의뢰로 실시한 맞춤형 연구 조사, *Assessing Organizations´Security Journeys*, 2023년 11월.

[4]Principled Technology 연구 결과는 인텔 기반 디바이스에만 제공됩니다.