DELL Technologies

최신 사이버 위협에 대처하는 방법

통합 엔드포인트 보안 및 관리 용이성

CROWDSTRIKE intel ABSOLUTE®

핵심 요약

새로운 공격 기법은 새로운 위험을 야기합니다. 여러 계층의 방어 수단이 함께 작동하여 최신 엔드포인트 위협에 미리 대비할 수 있습니다. 하드웨어 텔레메트리를 소프트웨어와 통합하여 광범위한 보안 및 관리 용이성을 개선하는 방법에 대해 알아보십시오. 관리가 간편한 디바이스와 솔루션으로 공격을 더욱 빠르게 차단하고 제로 트러스트(zero trust) 원칙을 지원하며 안전하게 혁신할 수 있습니다.

목차

위협 환경

사례 연구

2023년 Eclypsium은 타이완의 한 제조업체에서 판매하는 마더보드의 펌웨어에 결함이 있음을 발견했습니다. 그저 펌웨어를 최신 상태로 유지하려 했던 연구자들은 코드가 안전하지 않게 구현되어 메커니즘이 하이재킹되고 멀웨어 설치에 이용될 가능성이 있음을 알게 되었습니다.

이 발견이 경각심을 불러일으키는 몇 가지 이유

- 고객이 펌웨어 취약점을 통해 노출되었습니다.
- 이 취약점은 기존에 위협을 탐지하기 어려웠던 디바이스 영역에 존재했습니다.
- 자격 증명 검사를 우회하는 원격 공격을 시작하는 데 사용할 수 있습니다.

헤드라인에서 발췌...

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

Millions of PC Motherboards Were Sold With a Firmware Backdoor

수백 개의 마더보드 모델에 숨겨진 코드는 눈에 띄지 않으면서 보안을 약화시키는 방식으로 프로그램을 다운로드하는데, 이것이 악용되기 좋은 기능이라고 연구원들은 말합니다.

위협 환경

함의

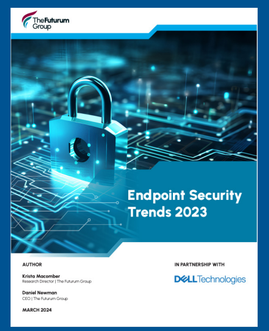
이는 IT 팀과 보안 팀의 우려를 낳는 주요 요인입니다.

디바이스 기반 공격.

공격자들은 이처럼 정교하고 악의적 공격을 통해 액세스 권한을 얻을 수 있습니다. 게다가 이 중 많은 공격은 바이러스 백신과 같이 기존 소프트웨어만을 사용한 보호 조치로는 완전히 감지하기 어렵습니다.

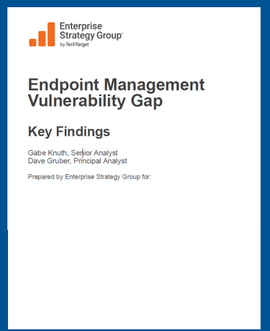
IT 및 보안 전문가를 대상으로 실시한 최근 글로벌 설문조사[1]에서 새로운 하드웨어 조달 시 조직이 가장 중요시하는 것으로 확인된 평가 기준:

BIOS 펌웨어 이벤트 탐지의 자동화



69%의 조직이 지난 12개월 이내에 최소 1건의 디바이스 수준 공격을 보고했습니다. 이는 2020년 연구보다 1.5배 더 높은 수치입니다![2]

고위험 구성



응답한 조직의 75% 이상은 알 수 없거나 관리되지 않거나 관리가 미흡한 엔드포인트 디바이스로 인해 발생하는 사이버 공격을 한 번 이상 경험했다고 보고했습니다.[3]

당면 과제

그렇다면 디바이스가 이렇게 공격하기 쉬운 대상이 되는 이유는 무엇일까요?

가시성

이러한 공격은 이전부터 가시성과 관찰 가능성이 결여되어 있었던 디바이스의 일부에서 발생하므로 찾아내기가 어렵습니다.

작업 능력

조직에서는 수십 개의 툴이 사일로에서 작동하는 경우가 많습니다. 따라서 공격이 탐지될 때 신속하게 대응하고 문제를 해결하는 것이 어려우며 이 과정에서 직접 처리해야 하는 일도 많습니다.

해결책

가시성

작업 능력

세계 최대의 기술 공급업체 중 하나인 Dell은 보안에 대해 많은 고민을 합니다. Dell에서 **가시성과 작업 능력을 우선시하는 PC를 구축하는 이유**가 여기에 있습니다. 이를 통해 IT 및 보안 운영 인력이 권한을 갖게 됩니다.

Dell PC에는 BIOS 검증[4] 및 공격 지표[4]와 같은 **고유한 보안 기능이 내장**되어 있어 피해가 발생하기 전에 위협을 사전에 탐지할 수 있습니다. 이렇게 탐지된 위협은 **Dell 전용 디바이스 텔레메트리**[4]를 통해 확인할 수 있습니다. 인텔 vPro® 기반의 Dell PC는 디바이스 수준에서 잠재적인 위협을 감지할 경우 그 내용을 운영 체제로 전송하므로 더 빠르고 효율적으로 조사하고 대응할 수 있습니다.

업계 리더십

우수한 보안을 자랑하는 Dell PC[4]

최신 위협에 대한 디바이스 신뢰를 유지하기 위해 무엇이 필요한지 알아보십시오.

디바이스 보안에 대한 Principled Technologies 연구 읽어보기 →


Principled Technologies®

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 equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

해결책

보안 및 관리 용이성을 통한 위협 대응

Dell 및 Dell 파트너 생태계는 작업 공간에서 가시성과 작업 능력을 발휘할 수 있도록 최선을 다하고 있습니다. 여기에는 다음이 포함됩니다.

- Dell의 공급망 보안과 내장 하드웨어 및 펌웨어 방어
- 인텔의 코어 실리콘 및 'OS 하위 계층' 보호
- Dell 및 통합 엔드포인트 관리 콘솔을 통한 관리 용이성
- CrowdStrike와 Absolute 등의 파트너와 협력하여 엔드포인트, 네트워크, 클라우드를 지능형 공격으로부터 보호합니다.

이 생태계는 IT와 보안 솔루션 사이의 간격을 좁히고 위협을 차단할 수 있도록 PC 텔레메트리를 커넥터로 사용합니다. 이러한 접근 방식은 공격을 방지하는 데 도움이 될 뿐만 아니라 공격을 탐지하고 이에 대응하여 복구 및 해결할 수도 있습니다.

활용 사례 및 대응책

통합 보안 및 관리 용이성으로 사이버 회복탄력성을 향상하는 방법을 설명하기 위해 공격 시나리오와 대응책을 비롯한 두 가지 활용 사례를 살펴보겠습니다.

먼저 BIOS 펌웨어에 대한 공격입니다. 여기서는 BIOS 다운그레이드 공격의 사이버 킬 체인[5]이 작용하는 방식을 알아봅니다.

BIOS 다운그레이드 공격

초기 액세스: 이동식 미디어 + 피싱을 통한 복제

1a 단계

악의적인 내부자는 기존 BIOS 취약점을 악용하여 OS 자격 증명을 원격으로 탈취할 수 있습니다. 디바이스를 해킹하고 BIOS를 다운그레이드합니다.

1b 단계

스피어 피싱 공격에 나선 공격자는 관리자가 악의적인 사이트에서 실수로 인증하면 세션 토큰을 탈취합니다.

2단계

자격 증명 액세스

공격자가 추가 관리자 계정을 만들어 지속성을 확보하고 네트워크를 통해 계속 이동합니다.

3단계

내부 이동

공격자가 네트워크를 매핑하고 시스템 관리 서버를 찾습니다.

4단계

데이터 유출

공격자가 웹 서비스를 통해 데이터를 유출합니다.

활용 사례 및 대응책

BIOS 다운그레이드 대응책

공격자들은 그 어느 때보다 빠르게 네트워크에 침입하고 있습니다. CrowdStrike의 Global Threat Report에 따르면 실제로 2023년 발생한 사이버 범죄의 평균 브레이크아웃 시간(시스템에 침입하여 측면 이동하는 데 걸리는 시간)은 2022년의 84분에서 62분으로 감소했습니다. 관찰된 최단 브레이크아웃 시간은 2분 7초에 불과했습니다![6]

Dell과 파트너인 인텔® 및 CrowdStrike가 하드웨어 지원 보안을 활용해 킬 체인을 따라 BIOS 다운그레이드 공격을 탐지하고 물리치는 방법을 소개합니다.

방지 | **탐지 및 대응** | **복구 및 개선**

안전한 공급망: 제공 과정에서 소싱과 어셈블리를 통해 설계 및 개발 중인 PC를 엄격한 제어로 보호할 수 있습니다. Dell과 인텔은 제품 수명 주기 전반에서 제품 취약성과 제품 변조의 위험을 완화하는 제품을 개발하기 위해 끊임없이 노력하고 있습니다.




Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

활용 사례 및 대응책

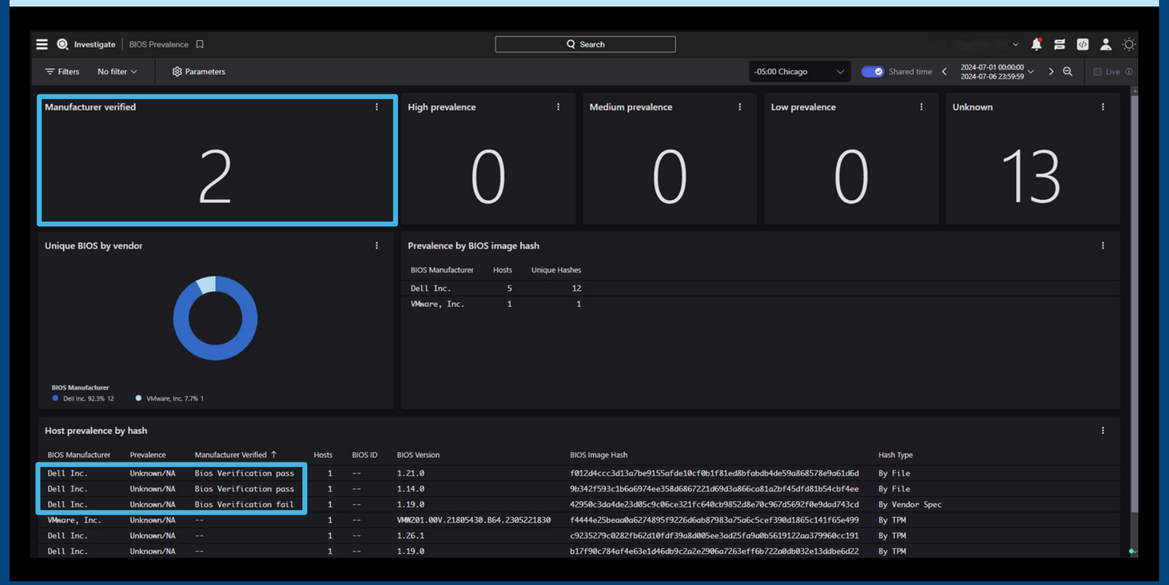
BIOS 다운그레이드 대응책

공격자들은 그 어느 때보다 빠르게 네트워크에 침입하고 있습니다. CrowdStrike의 Global Threat Report에 따르면 실제로 2023년 발생한 사이버 범죄의 평균 브레이크아웃 시간(시스템에 침입하여 측면 이동하는 데 걸리는 시간)은 2022년의 84분에서 62분으로 감소했습니다. 관찰된 최단 브레이크아웃 시간은 2분 7초에 불과했습니다![6]

Dell과 파트너인 인텔® 및 CrowdStrike가 하드웨어 지원 보안을 활용해 킬 체인을 따라 BIOS 다운그레이드 공격을 탐지하고 물리치는 방법을 소개합니다.

방지 | **탐지 및 대응** | 복구 및 개선

CrowdStrike Falcon 플랫폼에서 BIOS 증명 감지: Dell 디바이스 텔레메트리가 활성화되면 관리자는 BIOS 검증과 같은 기본 제공 보안 기능의 알림을 CrowdStrike Falcon에서 원격으로 확인할 수 있어 지속적인 침해가 발생하기 전에 의심스러운 활동을 빠르게 감지할 수 있습니다.



활용 사례 및 대응책

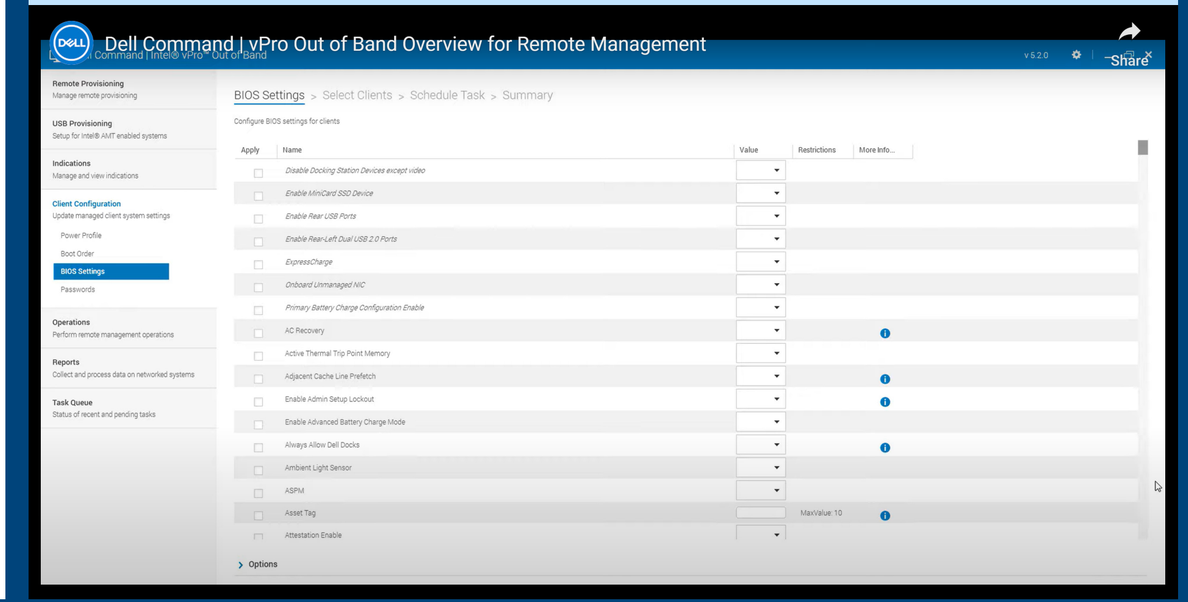
BIOS 다운그레이드 대응책

공격자들은 그 어느 때보다 빠르게 네트워크에 침입하고 있습니다. CrowdStrike의 Global Threat Report에 따르면 실제로 2023년 발생한 사이버 범죄의 평균 브레이크아웃 시간(시스템에 침입하여 측면 이동하는 데 걸리는 시간)은 2022년의 84분에서 62분으로 감소했습니다. 관찰된 최단 브레이크아웃 시간은 2분 7초에 불과했습니다![6]

Dell과 파트너인 인텔® 및 CrowdStrike가 하드웨어 지원 보안을 활용해 킬 체인을 따라 BIOS 다운그레이드 공격을 탐지하고 물리치는 방법을 소개합니다.

방지 | 탐지 및 대응 | **복구 및 개선**

BIOS 다운그레이드 해결: 아웃오브밴드(out-of-band) 시스템에 대한 향후 위협을 방지합니다. 인텔 vPro가 탑재된 Dell Client Command Suite는 원격 문제 해결을 지원합니다.



활용 사례 및 대응책

이 두 번째 활용 사례에서는 소프트웨어 공급망 공격의 킬 체인에서 단계가 진행되는 방식을 설명합니다.

소프트웨어 공급망 공격

1단계

초기 액세스: 공급망 침해

공격자가 소프트웨어 유틸리티(BIOS/펌웨어)에 악성 코드를 삽입.

2단계

지속성

고객이 디바이스를 업데이트하면서 악성 코드를 다운로드.

공격자가 멀웨어를 설치.

3단계

내부 이동

공격자가 방금 공격한 사용자를 스푸핑하고 다른 사용자에게 악성 링크를 전송. 해당 사용자가 링크를 클릭하면 공격자가 사용자의 자격 증명을 도용.

4단계

데이터 유출

공격자가 데이터를 유출합니다.

활용 사례 및 대응책

공급망은 공격자의 핵심 타겟이 되었습니다. 이러한 공격이 일반적이지는 않지만, 조직에서 해당 공격에 대한 방어 체계를 구축하는 방법을 아직 학습하는 단계이기 때문에 공격에 성공할 경우 그 결과는 파괴적일 수 있습니다.

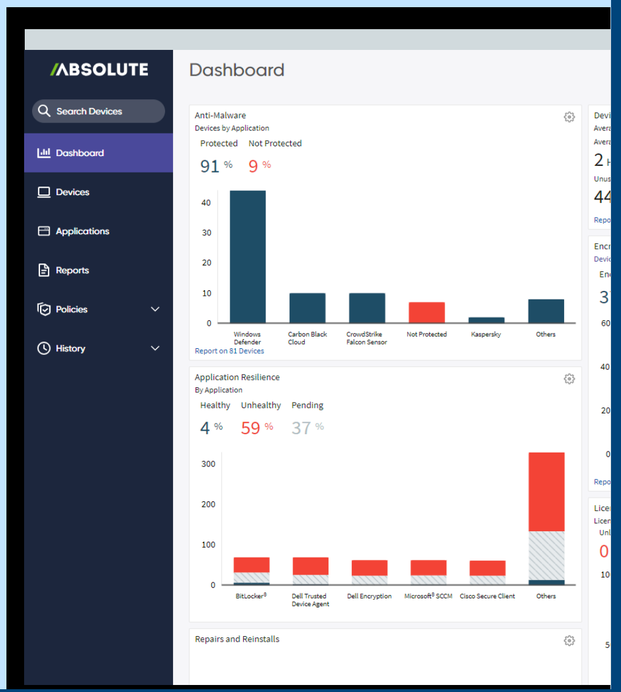
판매 중인 제품이 의도하지 않게 취약점을 통해 사용자에게 위험이 되지 않도록 방지하는 것은 모든 기술 공급업체의 중요한 책임입니다.

공격을 방지하고 보안 스택에 대한 회복탄력성을 확보하기 위해 Dell과 인텔®은 보안 개발 주기[7]의 엄격한 프로세스 및 프로토콜을 준수합니다. Dell Secured Component Verification[8]과 같이 추가적인 공급망 보증, Absolute의 펌웨어 수준 보안(오른쪽 그림 참조) 덕분에 고객은 PC의 수명 기간 내내 안심하고 제품을 사용할 수 있습니다.

방지 | 탐지 및 대응 | 복구 및 개선

공장의 엔드포인트 가시성: Dell에서 관리하는 공장에 Absolute가 내장되어 있어 네트워크 안팎의 모든 디바이스를 볼 수 있습니다. Absolute CFI(Custom Factory Install)는 배포 단계를 제거하여 창고 및 여러 최종 사용자 위치로 배송될 수 있는 디바이스를 보호합니다. 클라우드 기반 대시보드에서 전체 시스템을 확인하고 위험을 완화할 수 있습니다.

- IT 자산 및 애플리케이션의 전체 인벤토리를 손쉽게 찾고 유지 관리
- 전체 시스템을 찾아 매핑
- 자산 사용 최적화 및 보안 태세 모니터링
- 이기종 플랫폼 지원(Windows, Mac 및 Chrome)
- 27개 주요 PC OEM의 BIOS에 내장



활용 사례 및 대응책

공급망은 공격자의 핵심 타겟이 되었습니다. 이러한 공격이 일반적이지는 않지만, 조직에서 해당 공격에 대한 방어 체계를 구축하는 방법을 아직 학습하는 단계이기 때문에 공격에 성공할 경우 그 결과는 파괴적일 수 있습니다.

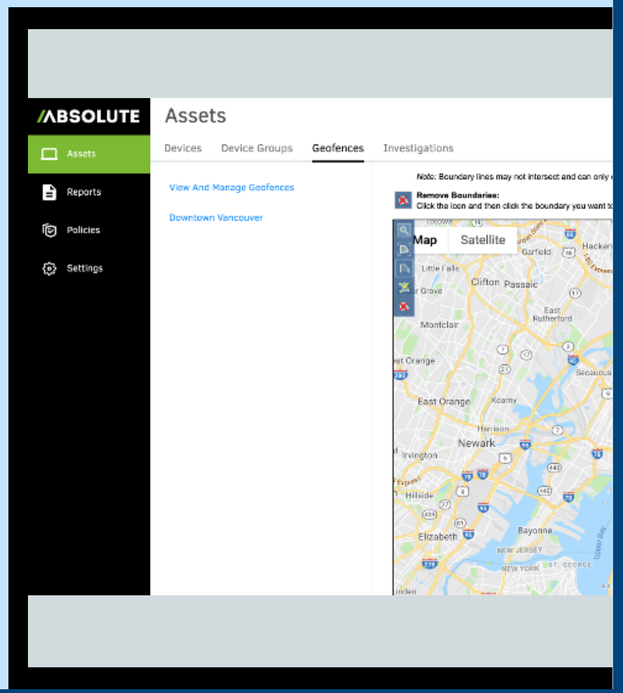
판매 중인 제품이 의도하지 않게 취약점을 통해 사용자에게 위험이 되지 않도록 방지하는 것은 모든 기술 공급업체의 중요한 책임입니다.

공격을 방지하고 보안 스택에 대한 회복탄력성을 확보하기 위해 Dell과 인텔®은 보안 개발 주기[7]의 엄격한 프로세스 및 프로토콜을 준수합니다. Dell Secured Component Verification[8]과 같이 추가적인 공급망 보증, Absolute의 펌웨어 수준 보안(오른쪽 그림 참조) 덕분에 고객은 PC의 수명 기간 내내 안심하고 제품을 사용할 수 있습니다.

방지 | **탐지 및 대응** | **복구 및 개선**

제어 엔드포인트: Absolute를 사용하여 엔드포인트가 손상된 시점을 감지합니다(예: 중요한 앱이 멀웨어에 의해 손상되거나 PC가 이동 중에 사라짐). 디바이스를 무용지물로 만들거나 포함된 데이터를 삭제하는 원격 조치를 통해 위협을 즉시 해결할 수 있습니다.

- 정의된 펜스 너머로 이동하는 디바이스 보호
- 중요한 데이터를 원격에서 보호 및 삭제
- 규정 준수 인증서로 EOL(End of Life) 데이터 삭제 수행
- 필요 시 중요한 자산을 보호하기 위한 디바이스 잠금
- 원격 펌웨어 보호 활성화



활용 사례 및 대응책

공급망은 공격자의 핵심 타겟이 되었습니다. 이러한 공격이 일반적이지는 않지만, 조직에서 해당 공격에 대한 방어 체계를 구축하는 방법을 아직 학습하는 단계이기 때문에 공격에 성공할 경우 그 결과는 파괴적일 수 있습니다.

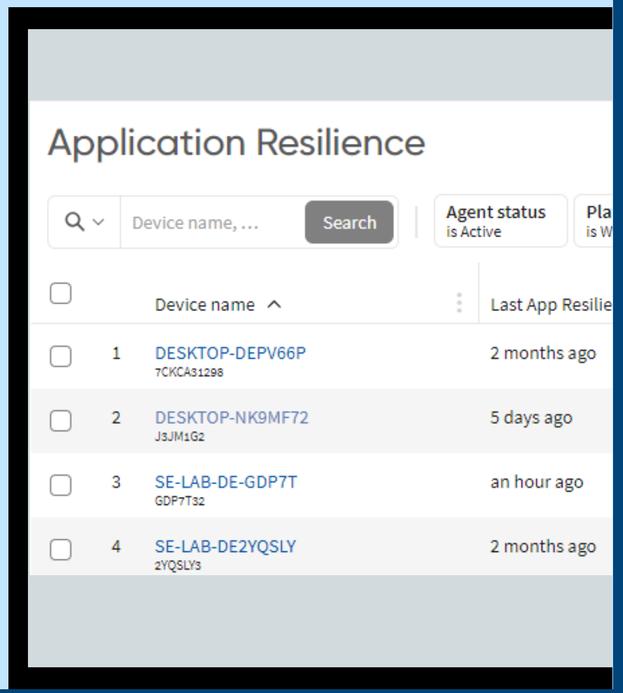
판매 중인 제품이 의도하지 않게 취약점을 통해 사용자에게 위험이 되지 않도록 방지하는 것은 모든 기술 공급업체의 중요한 책임입니다.

공격을 방지하고 보안 스택에 대한 회복탄력성을 확보하기 위해 Dell과 인텔®은 보안 개발 주기[7]의 엄격한 프로세스 및 프로토콜을 준수합니다. Dell Secured Component Verification[8]과 같이 추가적인 공급망 보증, Absolute의 펌웨어 수준 보안(오른쪽 그림 참조) 덕분에 고객은 PC의 수명 기간 내내 안심하고 제품을 사용할 수 있습니다.

방지 | **탐지 및 대응** | **복구 및 개선**

자체 복구: Dell BIOS 펌웨어에 Absolute Persistence가 내장되어 있어 무단 변경이 감지되면 원래 상태로 돌아갑니다. Absolute는 Dell Trusted Device Application, Zscaler 등의 기타 대응책 라이브러리가 포함된 Application Resilience 카탈로그(80개 이상의 애플리케이션)를 통해 손상된 엔드포인트 또는 지원되는 애플리케이션을 자체 복구하거나 유지할 수 있습니다.

- 엔드포인트에서 손쉽게 기밀 데이터를 찾아서 삭제
- 맞춤 구성된 스크립트 라이브러리를 통해 디바이스 전반에서 문제 해결 조치 수행
- 애플리케이션 모니터링 및 자가 복구
- 타사 엔드포인트 제어 기능으로 구성된 대규모 Application Resilience 카탈로그, 확장 중
- Absolute Investigations Team을 통해 분실 또는 도난된 디바이스를 찾아 조사



핵심 요점

시스템 전체의 보안은 개별 PC의 보안에 좌우됩니다.

최신 위협에 대처하려면 디바이스를 안전하게 구축해야 하며 보안 기능이 내장되어 있어야 합니다.

엔드포인트 보안 및 관리 용이성을 함께 적용하여 공격을 포착, 차단 및 복구합니다.

보안은 팀 스포츠와 같습니다. 최상의 방어를 위해 하드웨어와 소프트웨어를 모두 활용합니다.

자세히 보기:

문의: Global.Security.Sales@Dell.com

웹사이트: Dell.com/Endpoint-Security

팔로우: LinkedIn @DellTechnologies | X @DellTech

다음 단계

보안은 어떤 규모의 조직이든 어려운 주제입니다. **경험이 풍부한 보안 및 기술 파트너와 협력하여 엔드포인트 보안을 현대화하십시오.**

Dell Trusted Workspace는 최신 제로 트러스트 지원 IT 환경을 위한 엔드포인트 보안을 지원합니다. Dell만의 포괄적인 하드웨어 및 소프트웨어 보호 포트폴리오로 공격 노출 지점을 줄이십시오. Dell의 탁월하게 조율된 방어 기반 접근 방식은 내장된 보호 기능과 지속적인 경계 상태를 결합하여 위협을 상쇄합니다. 사용자는 생산성을 유지하고, IT 담당자는 오늘날의 클라우드 기반 환경을 위해 구축된 보안 솔루션으로 언제나 안심할 수 있습니다.

1. 출처: TechTarget 부서인 Enterprise Strategy Group이 Dell Technologies 의뢰로 실시한 맞춤형 연구 조사, *Assessing Organizations ´Security Journeys*, 2023년 11월.
2. 출처: Futurum Group, Endpoint Security Trends, 2023년.
3. 출처: TechTarget 부서인 Enterprise Strategy Group의 연구 보고서, *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, 2023년 5월.
4. Dell 내부 분석 기준, 2024년 10월. 인텔 프로세서를 탑재한 PC에 해당합니다. 일부 기능을 지원하지 않는 PC도 있습니다. 일부 기능의 경우 별도로 구매해야 합니다. Principled Technologies의 검증을 받았습니다. A comparison of security features, 2024년 4월.
5. 출처: What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. 출처: CrowdStrike 2024 Global Threat Report.
7. 출처: Three Considerations for Establishing Device Trust | Dell USA.
8. 출처: How to Keep Device Trust Close to the Vest | Dell USA.