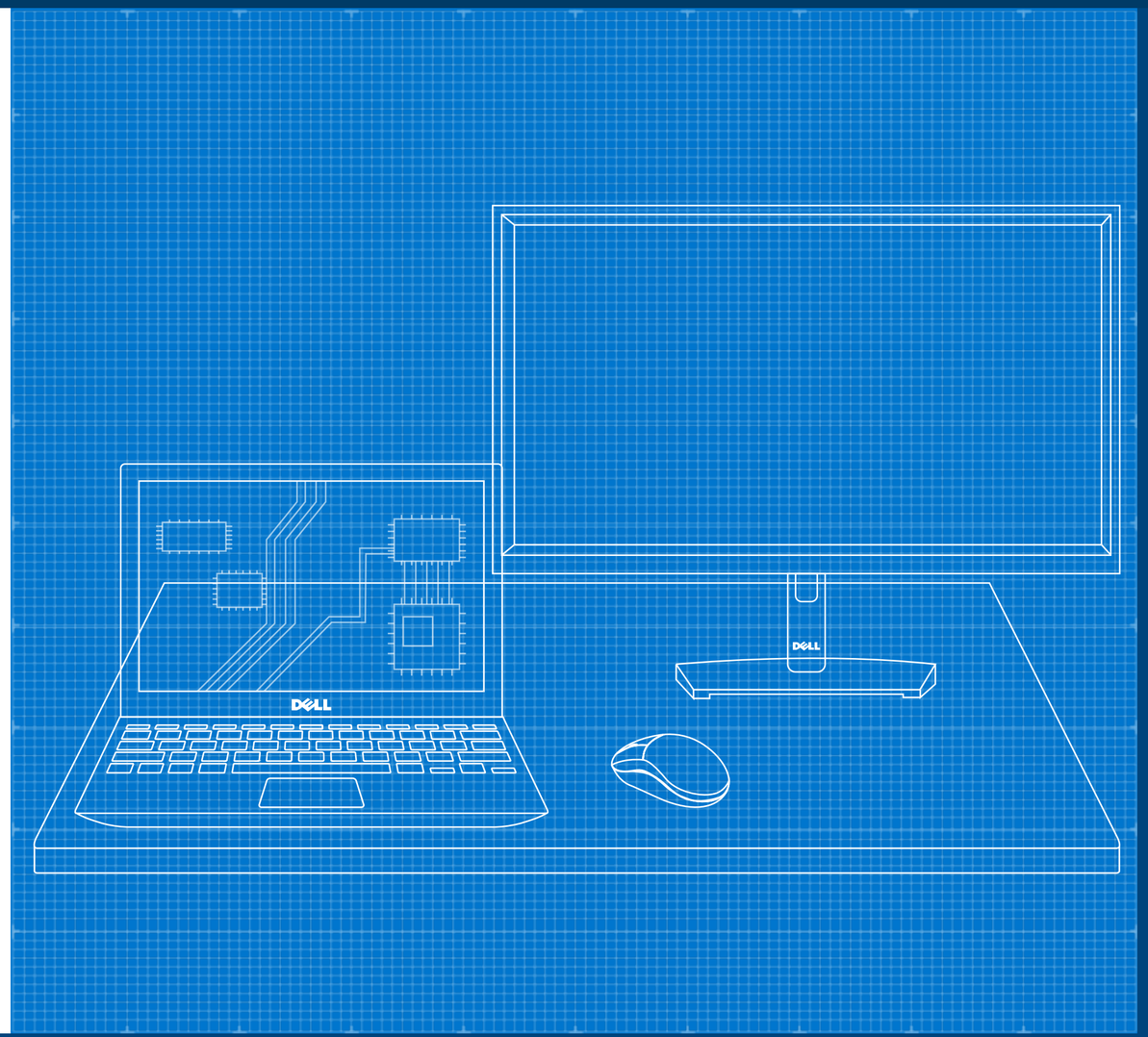
DELL Technologies

신뢰할 수 있는 업무 환경의 구조

다중 계층 방어 체계를 통해 전체 시스템의 보안 강화



DELL Technologies

핵심 요약

사이버 공격은 피할 수 없는 현실이며, 그 규모와 교묘함이 점점 더 커지고 있습니다. 엔드포인트 디바이스, 네트워크, 클라우드 환경이 공격의 주요 표적으로 떠올랐습니다.

이 eBook에서는 계속 진화하는 위협 환경에서 가장 효과적으로 엔드포인트를 방어하는 데 필요한 요소에 관한 지침을 IT 및 보안 의사 결정권자에게 제공합니다.

목차

위협 환경

하이브리드 근무 방식으로 전환되면서 새로운 복잡성 및 공격 벡터가 생겨났고 **엔드포인트와 네트워크, 클라우드로 인해 공격 노출 지점이 확장되고 있습니다.**

더욱이 공격자들은 이제 컴퓨팅 스택의 여러 계층을 표적으로 삼아 유효한 시스템 프로세스에 섞여 드는 교묘한 공격 기법을 사용하고 있습니다. 공격자가 *전혀 탐지되지 않으면서* 액세스 권한을 획득하여 소프트웨어 보호 기능을 비활성화할 수 있는 방법도 있습니다.

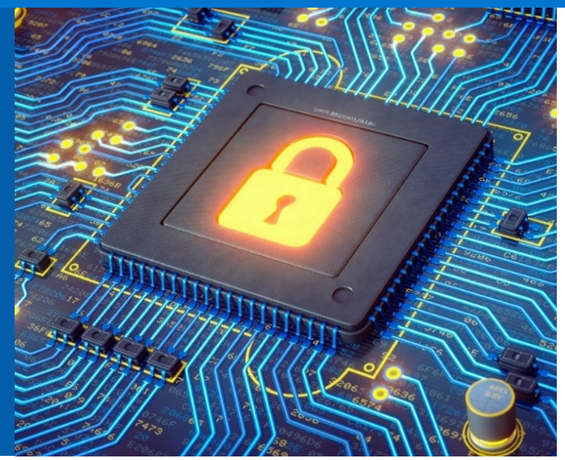
많은 조직이 이러한 위협과 싸우기 위해 제로 트러스트(Zero Trust) 여정에 착수했습니다. 하지만 제로 트러스트 원칙을 적용하려면 디바이스의 신뢰성을 유지할 수 있어야 합니다.

공격이 더욱 빈번해지고 첨단 기술 때문에 새로운 공격 벡터가 생겨나는 상황에서 **디바이스 신뢰성을 어떻게 유지할 수 있을까요?**

[1]CrowdStrike Global Threat Report, 2024년.
[2]Dell Innovation Index, 2023년.

알고 계셨습니까?

2023년 공격의 75%는 멀웨어 기반이 아니었습니다.[1]



설문조사에 참여한 조직 중 불과 41%만이 기술과 애플리케이션에 보안 기능이 내장되어 있다고 매우 자신 있게 말할 수 있습니다.[2]

사이버 보안 성숙도를 높이기 위해 제로 트러스트에 대해 알아보고 계십니까?
eBook 확인: *제로 트러스트 여정의 필수 요소, 엔드포인트 보안*.

당면 과제

효과적인 엔드포인트 보안을 위해 공격자와 그들의 공격 방식을 이해해야 합니다.

보안 침해로 얻을 수 있는 보상금 때문에 **공격자는 한 조직에 여러 차례 침입을 시도하면서 다양한 방법과 진입 지점을 활용하여 확률을 높이는 경우가 많습니다.** 예를 들어, 단일 디바이스의 수명주기 동안 공격자는 수십 가지 벡터를 통해 취약성을 이용하려고 시도할 수 있습니다.

기존 방어 체계는 엔드포인트의 보안을 유지하기에 충분하지 않습니다. 조직에서 하나의 공격 노출 지점을 강화하면 위협 행위자는 더 약한 표적으로 옮겨갈 뿐입니다. 전 세계가 하이브리드 방식으로 전환되면서 위협 행위자는 엄청난 피해로 이어진 새로운 엔드포인트 공격 벡터를 파악했습니다.

오른쪽의 공격 예시 확인

공급망 공격: 공급업체를 표적으로 삼아 공급업체 그리고 더 나아가 해당 고객의 시스템, 데이터, 네트워크에 대한 액세스 권한을 획득합니다. **예: 구성 요소 변조로 시작되는 하드웨어 공급망 공격:**

공격자가 PC 화물을 가로채 하드 드라이브를 변경합니다.

IT 부서가 회사 전체에 보안이 침해된 디바이스를 배포합니다.

공격자가 멀웨어를 설치하여 사용자가 로그인할 때 자격 증명을 추출합니다.

소셜 엔지니어링 공격: 사용자를 속여 디바이스 및 네트워크 액세스 권한을 획득하는 데 사용할 수 있는 기밀 정보를 얻습니다. **예: 피싱 이메일로 시작되는 스푸핑 공격:**

사용자가 피싱 이메일에 속아 스푸핑된 웹페이지에서 자격 증명을 넘깁니다.

공격자가 유효한 자격 증명을 사용하여 네트워크에 원격으로 액세스합니다.

공격자가 웹 서비스를 통해 데이터를 무단으로 반출하고 훔친 데이터를 암호화하고 이를 볼모로 대가를 요구합니다.

현대적인 업무 환경 확보

PC의 구매와 제조부터 배송, 배포, 사용과 퇴역까지, **엔드포인트 보호를 위해서는 디바이스 수명주기 전반의 다양한 상태에서 방지, 탐지 및 대응, 복구 및 문제 해결 작업이 필요합니다.** 이러한 모든 공격 노출 지점이 결합된 규모를 상상해 보십시오!

가장 효과적인 사이버 보안 전략은 최악의 시나리오에 대비해 계획을 세우는 것입니다. 보안 침해가 발생할 수 있다고 가정하고 여러 계층의 보호 기능을 갖춰 가능한 한 빨리, 최대한 자주 공격을 차단해야 합니다. 또한 반복적인 침해 위험을 최소화하기 위한 문제 해결 기능도 포함합니다.

방지

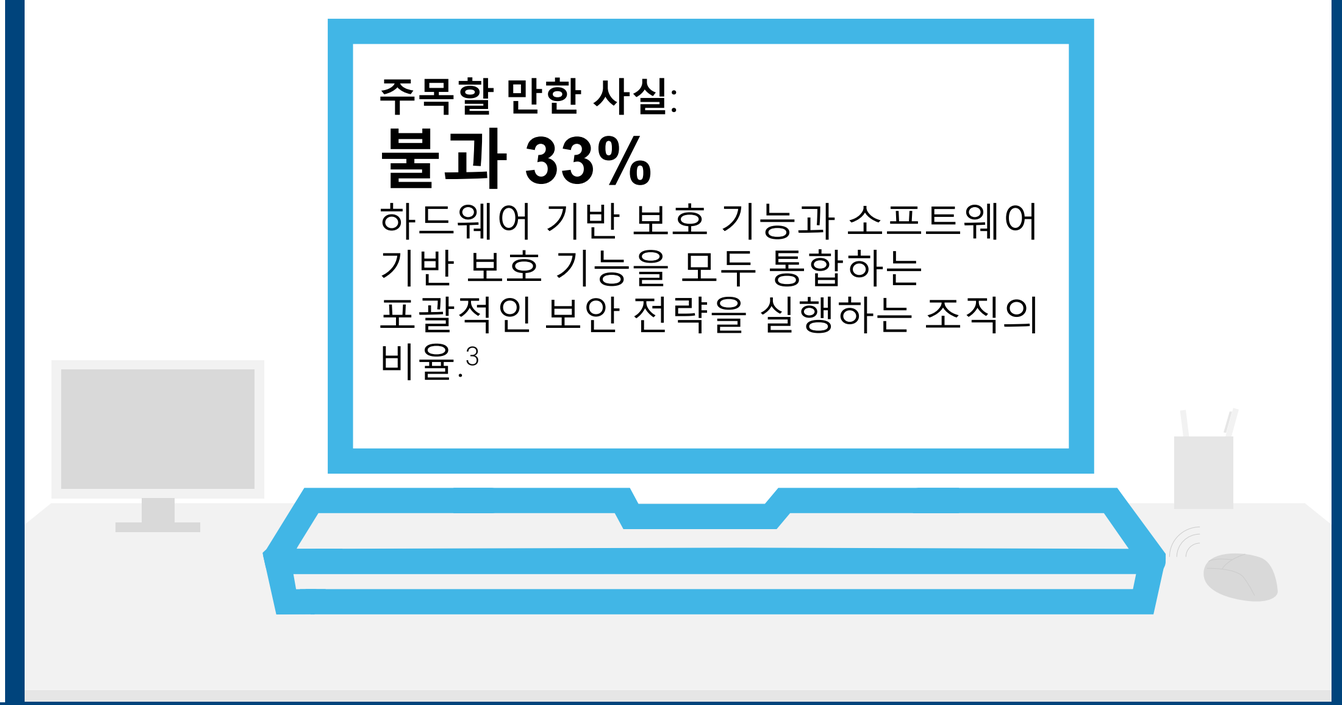
공격을 차단하도록 설계된 방어 기능을 활용하여 공격 노출 지점을 줄입니다.

탐지 및 대응

항상 보안 침해를 염두에 두고 경계 상태를 유지합니다.

복구 및 문제 해결

공격의 영향을 완화하고 일상 업무 상태로 돌아갑니다.



[3]Dell Innovation Index, 2023년.

신뢰할 수 있는 업무 환경의 구조

최신 엔드포인트 보안에는 다음 세 가지가 필요합니다.

1. **소프트웨어 보안:** 오늘날에는 기업 네트워크 외부의 사용자와 디바이스, 데이터를 그 어느 때보다 많이 볼 수 있습니다. 소프트웨어 보안은 디바이스를 보호할 뿐 아니라 악의적인 활동이 자주 발생하는 네트워크 및 클라우드 환경까지 보호합니다.

2. **하드웨어 보안:** 디바이스에는 보안 기능이 내장되어 있어야 합니다. 이는 사용 중인 디바이스를 보호하는 하드웨어 및 펌웨어 보안과 관련됩니다. 업무 환경을 보호하려면 디바이스에 대한 가시성과 제어력을 제공하는 기능이 내장되어 있어야 합니다.

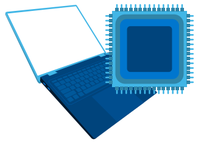
3. **공급망 보안:** 디바이스는 안전하게 제작되어야 합니다. 즉, a) 위협 환경을 이해하고 b) 그 지식을 진화하는 위협 환경에 맞춰 활용할 수 있는 공급업체와 협력해야 합니다. 안전한 PC 설계, 개발 및 테스트로 제품 취약성의 위험을 최소화하고, 공급망 제어를 통해 제품 변조 위험을 완화합니다.

다중 보안 계층 살펴보기

(보안 조치의 대표적인 예 목록)

소프트웨어 보안

- NGAV(Next-Gen Antivirus)
- EDR(Endpoint Detection and Response)
- XDR(Extended Detection and Response)
- 클라우드 데이터 보호
- 네트워크 보호
- 자동화된 자가 복구



하드웨어 및 펌웨어 보안

- 부팅 시 검증
- 런타임 검증
- 사용자 인증
- 보안 알림 및 경고/텔레메트리

공급망 보안

- 보안 개발 방식 운영
- 보안 공급망 운영
- 구성 요소 검증
- 변조 식별 패키징

Dell의 접근 방식: Dell Trusted Workspace

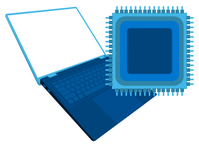
Dell은 전 세계 조직을 위한 보안 및 IT 파트너입니다. 포인트 솔루션과 달리, Dell은 전반적인 보안 성과에 초점을 맞춰 킬 체인을 차단하고 사이버 공격에 대한 회복탄력성을 강화하는 솔루션 제품군을 구축합니다. **Dell Trusted Workspace에는 다음이 포함됩니다.**

- 우수한 보안을 자랑하는 PC를 제작하는 Dell 고유의 **하드웨어 및 펌웨어 보호 기능.**[4]*(기본 구축 및 내장 보안 기능)*
- 디바이스, 네트워크, 클라우드에 대한 지능형 공격을 방어하는, **업계를 선도하는 소프트웨어** 파트너 생태계. *(추가 구축 보안 기능)*

[4]Dell 내부 분석 기준, 2024년 10월. 인텔 프로세서를 탑재한 PC에 해당됩니다. 일부 기능을 지원하지 않는 PC도 있습니다. 일부 기능의 경우 별도로 구매해야 합니다. Principled Technologies의 검증을 받았습니다. A comparison of security features, 2024년 4월.

추가 구축(Built-*on*) 파트너 생태계가 제공하는 소프트웨어 보안

- **Dell SafeGuard and Response: CrowdStrike** 및 **Secureworks**는 위협을 탐지 및 대응하고 문제를 해결합니다.
- **Dell SafeData: Netskope**는 클라우드 기반 앱을 위한 가시성, 모니터링, 데이터 손실 방지 기능을 제공합니다. **Absolute**는 앱과 네트워크를 자가 복구하는 기능을 활성화합니다.



기본 내장 우수한 보안을 자랑하는 PC를 통한 하드웨어 및 펌웨어 보안[4]

사용 중인 디바이스 보호 기능 예시:

- **Dell SafeBIOS** 오프 호스트 BIOS 검증*, IoA(Indicators of Attack)* 및 CVE 탐지*는 PC의 보안이 침해되기 전에 악성 활동을 탐지하는 데 도움이 됩니다.
- **Dell SafeID**는 전용 보안 칩으로 사용자 자격 증명을 보호합니다.*
- **오프 호스트 펌웨어** 검증은 권한이 높은 펌웨어의 무결성을 보호합니다.*
- **Dell은 Dell Trusted Device 앱**을 통해 디바이스 텔레메트리와 업계를 선도하는 소프트웨어를 통합하여 전체 시스템의 보안을 강화합니다.*

기본 구축(Built-*with*) 공급망 보안으로 처음 부팅할 때부터 PC의 보안 보장

- Dell의 SCV(Secured Component Verification)*와 같은 **Dell SafeSupply Chain** 추가 기능은 제품 무결성을 추가적으로 보증합니다.

** Dell 고유 기능*

Dell과 함께 종합적인 솔루션 구현

하드웨어 및 소프트웨어 대응책을 모두 갖추고, 일반적인 공격을 방지하는 데 도움이 되는 방어 체계를 통해 공격 노출 지점을 줄입니다.

공격이 교묘하게 빠져나가지 못하도록 탐지 및 대응 기능으로 처리합니다.

4페이지에서 살펴본 공급망 공격의 경우, Dell과 협력하면 **보안 공급망 운영**과 같은 사전 예방적인 조치로 킬 체인 초기에 공격을 차단할 수 있습니다. 교묘하게 빠져나가는 공격에 대비해 **SCV**와 같은 추가 대응책도 마련되어 있습니다.

소셜 엔지니어링 공격의 경우, 공격자가 사용자를 속여 유효한 자격 증명을 획득하더라도 **SafeID와 같은 하드웨어 기반의 사용자 검증**을 통해 공격자의 접근을 즉시 차단하고 추가 액세스를 거부할 수 있습니다. **차세대 보안 웹 게이트웨이**와 같은 보안 소프트웨어는 추가적인 모니터링 보호 계층을 제공할 수 있습니다.

구성 요소 변조로 시작되는 하드웨어 공급망 공격에 대응합니다.

공격자가 PC 화물을 가로채 하드 드라이브를 변경합니다.

- **보안 공급망 운영**
- 변조 식별 패키징
- 도어 잠금 장치

IT 부서가 회사 전체에 보안이 침해된 디바이스를 배포합니다.

- SCV(Secured Component Verification)
- 런타임 검증

공격자가 멀웨어를 설치하여 사용자가 로그인할 때 자격 증명을 추출합니다.

- 클라우드 액세스 보안 브로커
- 차세대 보안 웹 게이트웨이

피싱 이메일로 시작되는 소셜 엔지니어링 공격에 대응합니다.

사용자가 피싱 이메일에 속아 스푸핑된 웹페이지에서 자격 증명을 넘깁니다.

- NGAV
- EDR
- XDR

공격자가 유효한 자격 증명을 사용하여 네트워크에 원격으로 액세스합니다.

- SafeID를 통한 다단계 인증
- 제로 트러스트 네트워크 액세스

공격자가 웹 서비스를 통해 데이터를 무단으로 반출하고 훔친 데이터를 암호화하고 이를 볼모로 대가를 요구합니다.

- 차세대 보안 웹 게이트웨이 + 사용자 개체 동작 분석

핵심 요점

보안 침해는 피할 수 없는 현실입니다. 효과적인 엔드포인트 보안은 항상 최악의 시나리오를 가정하고 디바이스부터 네트워크와 클라우드에 이르기까지 킬 체인이 어디에서 발생하든 킬 체인을 차단하는 데 초점을 맞춥니다.

하나의 솔루션으로 모든 공격을 100% 차단할 수는 없습니다. 하드웨어 대응책과 소프트웨어 대응책을 결합하여 최상의 방어 체계를 구축하십시오.

보안을 강화하기 위해서는 공급업체의 보안도 강화해야 합니다. 공급업체에 현재 운영 중인 보안 조치를 간략히 설명해 달라고 요청해 보십시오.

Latitude 노트북 및 2-in-1 PC

자세한 정보:

문의: Global.Security.Sales@Dell.com

웹사이트: Dell.com/Endpoint-Security

소셜 미디어: 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.