DELL Technologies

제로 트러스트 여정의 필수 요소, 엔드포인트 보안

제로 트러스트 준비를 위한 세 가지 권장 사항

DELL Technologies

핵심 요약

제로 트러스트 달성은 장기적인 여정입니다. 제로 트러스트는 조직에서 구현하는 제품이나 솔루션이 아니라 시간이 지남에 따라 구축되는 보안 관리를 위한 전략적 프레임워크입니다. 이 eBook에는 제로 트러스트 혁신을 탐색하는 IT 의사 결정권자를 위한 실질적인 지침이 나와 있습니다. 특히 지금처럼 어디서나 업무가 가능한 세계에서 엔드포인트 디바이스 보안이 현대적이고 안전한 기반을 다지기 위해 수행하는 역할에 초점을 맞추고 있습니다.

목차

통합의 사이버 현황 3
어디서나 업무가 가능한 세계의 시사점 4
변화가 필요한 보안 전략 5
제로 트러스트의 기본 원리 이해 6
제로 트러스트 원칙 활성화 7
제로 트러스트 준비를 위한 세 가지 권장 사항 8
핵심 요점 11
다음 단계 11

통합의 사이버 현황

점차 원격/하이브리드 및 클라우드 근무 환경으로 전환함에 따라 보안 위협이 증가하고 있습니다.

조직의 데이터 자산을 보호하는 작업의 복잡성은 지난 몇 년 동안 엄청나게 증가했습니다. 원격 근무/하이브리드 근무 수요가 늘어나면서 클라우드를 통해 비즈니스 생산성을 높일 수 있었지만, 그에 따른 위험도 증가하고 있습니다. 온프레미스 인프라스트럭처만 관리하던 방식에서 클라우드를 포괄하는 방식으로 전환함에 따라 공격자들에게 노출되는 공격 지점이 확대되었으며, 그에 따른 결과의 영향도 커졌습니다. 예를 들어 공격자가 공격에 성공하면 단지 한 고객만이 아니라 잠재적으로 해당 클라우드 서비스의 모든 고객과 공급망 전체의 고객에게 영향을 미칠 수 있습니다. 국가이든 일반 범죄자이든 위협 행위자로 인해 치러야 할 대가는 막대할 수 있으며 결과적으로 이들은 악용할 새로운 취약성을 계속해서 찾을 것입니다.

사이버 범죄로 인한 전 세계 피해 비용은 **2025년까지 10조 5,000억 달러**로 증가할 것으로 예상됩니다.[i]

Verizon이 한 2022년 연구에서 보고한 확인된 데이터 침해 횟수는 **5,200**회에 달했으며, 이는 **전년도에 비해 1.3배 증가한 수치**입니다.[ii]

어디서나 업무가 가능한 세계의 시사점

조직은 진화하는 위협 환경을 극복할 수 있는 방법을 찾아야 합니다.

그렇다면 점점 더 재택/원격 근무로 전환되는 세계에는 어떤 시사점이 있을까요? 다음과 같은 두 가지로 요약됩니다.

모든 조직이 취약해집니다.

"목적이 분명한 어떤 단체가 진심으로 여러분의 시스템에 침입하고자 한다면 성공할 확률이 정말 높습니다."

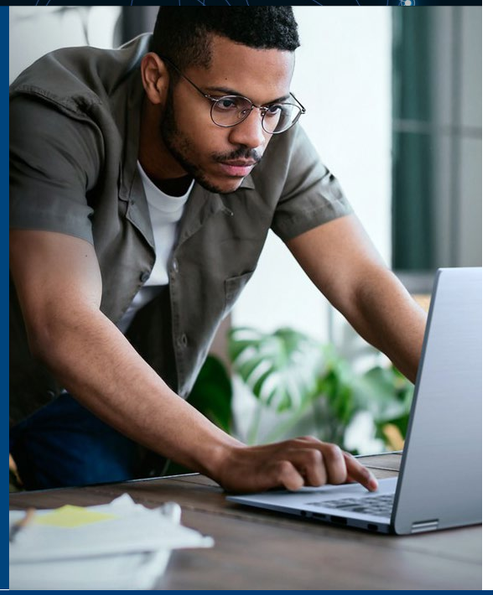
— Michael Rogers 제독, 전 미국 국가안보국 국장이자 전 미국 사이버사령부 사령관[iii]

그리고 잘못되는 경우 매우 큰 대가를 치러야 할 수 있습니다.

"2022년 데이터 침해로 인한 비용은 사상 최고치를 기록한 평균 435만 달러였습니다[2020년보다 12.7% 증가]."[iv]

공격 벡터가 증가하고 공격 지점이 확대됨에 따라 그 어떤 회사의 보안도 완벽할 수 없습니다. 조직은 최악의 시나리오를 가정하고 불가피한 공격에 대한 방어를 강화해야 합니다.

조직의 69%는 제대로 관리되지 않은 인터넷 연결 자산으로 인해 일종의 사이버 공격을 경험했습니다.[v]



진화가 필요한 보안 전략

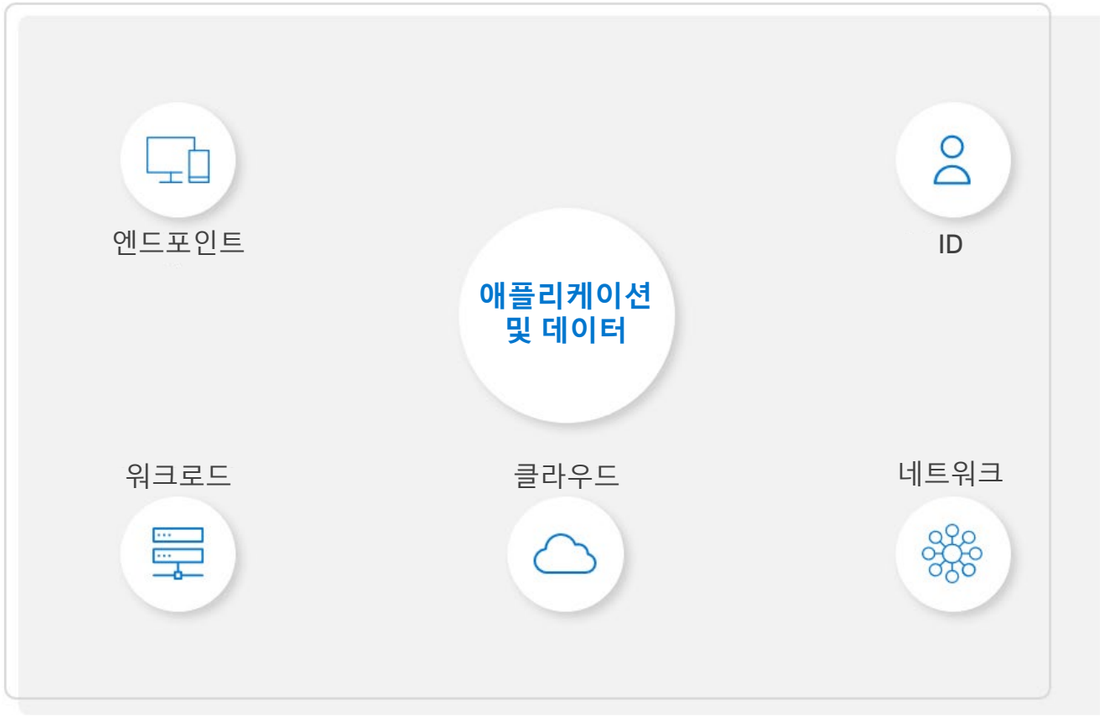
클라우드 기반 환경을 수용해야 합니다. 이에 대한 해답이 바로 제로 트러스트입니다.

기존의 보안 모델로는 더 이상 효과를 볼 수 없습니다. 그 이유는 다음과 같습니다.

어떤 조직이든 효과적인 보안 태세를 갖추려면 5가지 제어 지점, 즉 엔드포인트, 워크로드, ID, 네트워크 및 클라우드를 고려해야 합니다. 목표는 애플리케이션과 데이터를 보호하는 것입니다.

기존 접근 방식은 사일로화되어 있는 경우가 많으며, 이러한 방식을 사용하는 조직은 공격에 더 취약합니다.

다음...

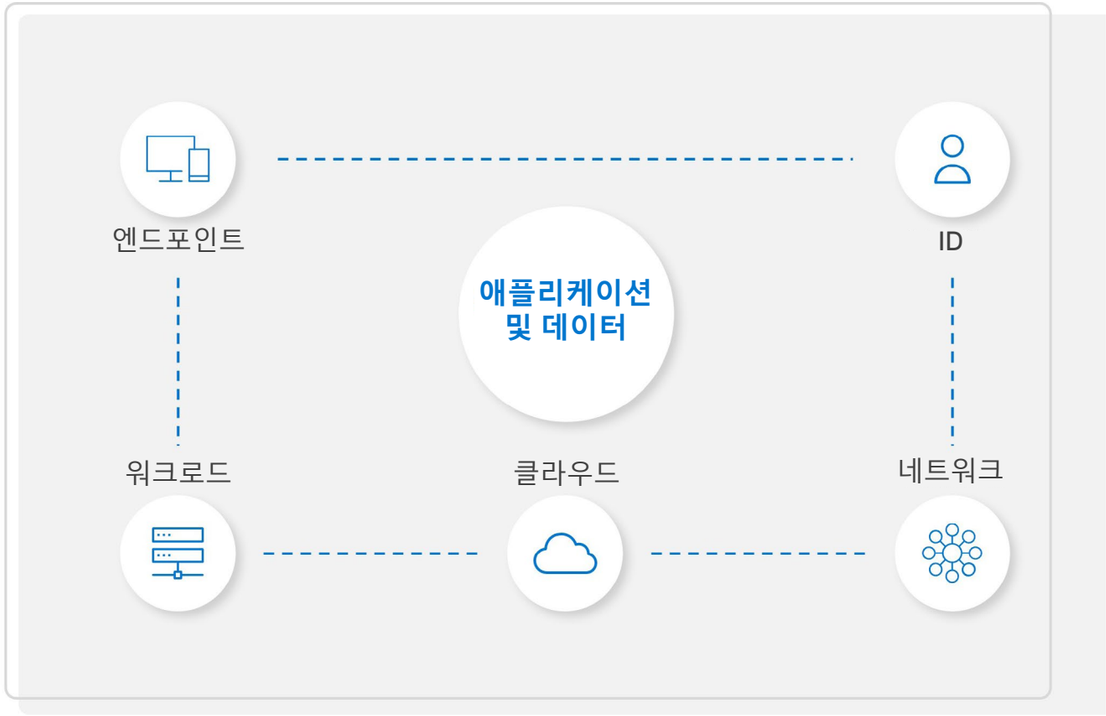


진화가 필요한 보안 전략

클라우드 기반 환경을 수용해야 합니다. 이에 대한 해답이 바로 제로 트러스트입니다.

현대적인 접근 방식은 제어 지점 간의 통신을 개선하여 제어 역량을 더욱 확대하는 방향으로 발전했습니다. 그러나 원격 근무/하이브리드 근무 환경을 도입하는 경우가 점차 늘고 있으므로 이에 따라 경계를 더욱 강화해야 합니다.

다음...

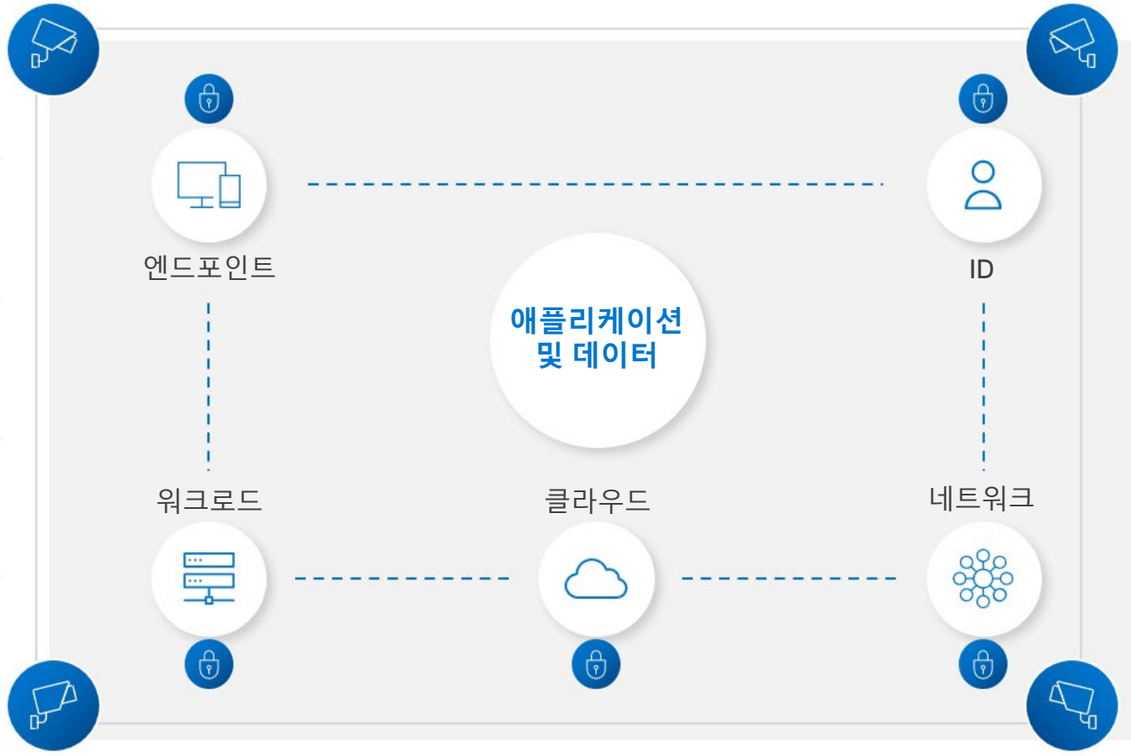


진화가 필요한 보안 전략

클라우드 기반 환경을 수용해야 합니다. 이에 대한 해답이 바로 제로 트러스트입니다.

오늘날 직원들은 집, 카페, 호텔 등 어디서나 업무를 수행합니다. 이들은 방화벽으로 보호된 사무실 및 데이터 센터와의 연결이 제한되거나 불가능하고 안전하지 않은 Wi-Fi를 사용하는 경우가 많습니다. 기본적인 활용 방식은 디바이스에서 인터넷에 직접 연결하여 클라우드 파일 서버와 SaaS(Software as-a-Service) 애플리케이션에 연결하고 엔터프라이즈 데이터로 작업하는 것일 수 있습니다.

공격이 점점 더 정교해지고 공격 벡터가 증가함에 따라 암묵적 신뢰를 기반으로 하는 기존의 보안 전략은 더 이상 효과적이지 않습니다. 이에 대한 해답이 바로 제로 트러스트입니다.

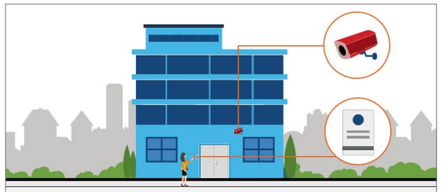


제로 트러스트의 기본 원리 이해

제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.



직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.

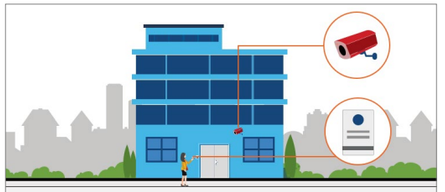
다음...

제로 트러스트의 기본 원리 이해

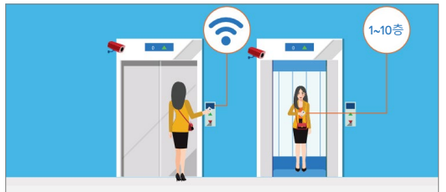
제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.



직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.



직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

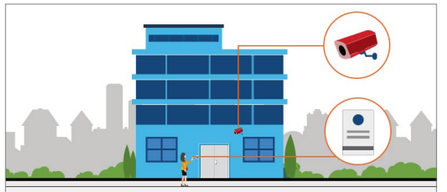
다음...

제로 트러스트의 기본 원리 이해

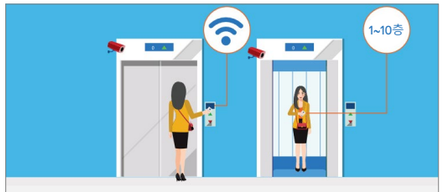
제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.



직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.



직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

직원은 다시 배지를 사용해 엘리베이터의 층 선택 기능을 활성화합니다.

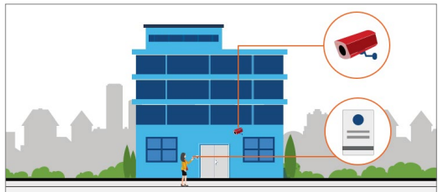
다음...

제로 트러스트의 기본 원리 이해

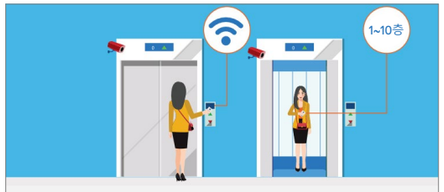
제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.

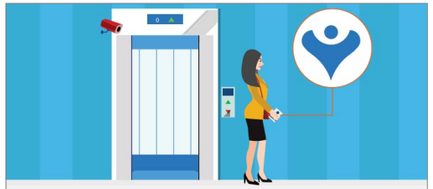


직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.



직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

직원은 다시 배지를 사용해 엘리베이터의 층 선택 기능을 활성화합니다.



원하는 층에 도착하면 직원의 사무 공간으로 걸어서 이동합니다.

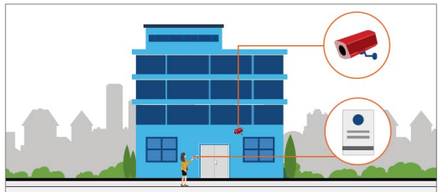
다음...

제로 트러스트의 기본 원리 이해

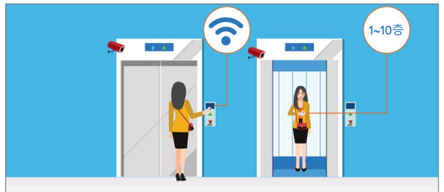
제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.

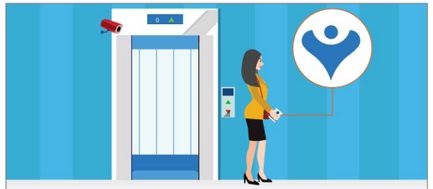


직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.

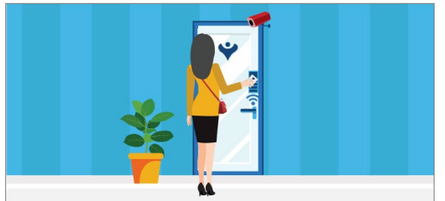


직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

직원은 다시 배지를 사용해 엘리베이터의 층 선택 기능을 활성화합니다.



원하는 층에 도착하면 직원의 사무 공간으로 걸어서 이동합니다.



ID 카드를 사용해 본인의 사무 공간에 들어갑니다.

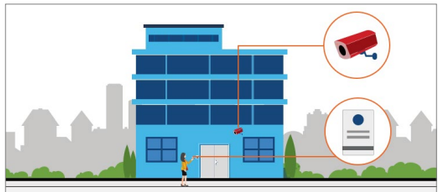
다음...

제로 트러스트의 기본 원리 이해

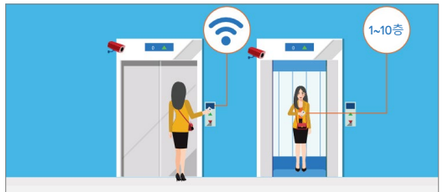
제로 트러스트는 보안에 관한 새로운 사고 방식입니다. 이 개념은 암묵적 신뢰를 대체합니다. 즉, 사용자가 인증을 완료한 후에 네트워크를 자유롭게 탐색할 수 있게 합니다. 제로 트러스트는 패러다임을 뒤집어 조직이 IT 환경을 명시적으로 제어할 수 있도록 합니다.

보안 프로토콜 구축이라는 잘 알려진 개념으로 제로 트러스트를 설명해 보겠습니다.

여러분은 회사 사무실에서 일합니다. 채용 시 배지를 받고 보안 프로토콜을 숙지했습니다. 매일 회사 건물에 들어가며, 건물에는 카메라가 사방에 설치되어 있습니다. 여러 지점에서 배지 확인을 거치고 책상에 앉으면 비밀번호를 입력해 컴퓨터의 잠금을 해제합니다.

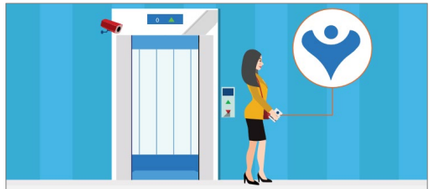


직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.

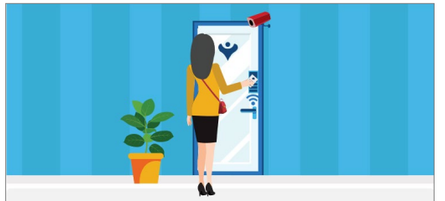


직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

직원은 다시 배지를 사용해 엘리베이터의 층 선택 기능을 활성화합니다.



원하는 층에 도착하면 직원의 사무 공간으로 걸어서 이동합니다.



ID 카드를 사용해 본인의 사무 공간에 들어갑니다.

직원이 본인의 책상에 앉으면 비밀번호를 사용해 컴퓨터의 잠금을 해제합니다.

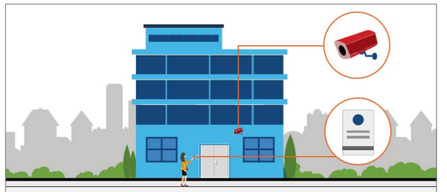
다음...

제로 트러스트의 기본 원리 이해

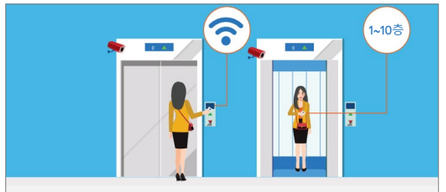
이것이 바로 제로 트러스트의 작동 원리입니다.

고용주는 입사 첫날에 여러분의 신원을 확인합니다. 그 이후로 여러분이 요청하는 모든 액세스는 조직의 자산(사용자, 데이터 등)을 보호하기 위해 검증을 거칩니다. 보안을 강화하기 위해 보안 요원들은 건물 내의 모든 움직임을 모니터로 감시합니다. 모든 이상한 행동(예: 액세스해서는 안 되는 제품군에 액세스하려는 시도)은 조사 대상이 됩니다.

오늘날 우리는 그 어느 때보다 빈번하게 회사 네트워크 외부에서 사용자, 디바이스, 앱 및 데이터를 찾고 있습니다. 결과적으로 사용자 ID는 사각지대가 되었으며 ID 손상은 대부분의 침해에서 핵심 요소가 됩니다. 제로 트러스트 과정은 이를 바로잡습니다.

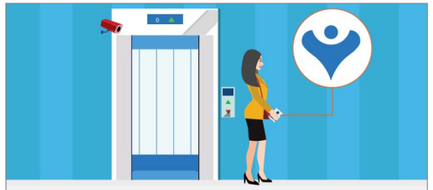


직원이 사무실 건물에 도착한 후 배지를 꺼내 건물에 들어갑니다.

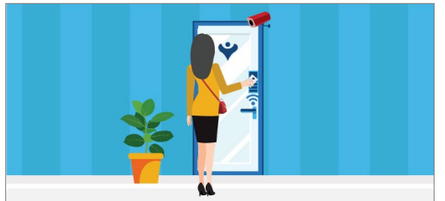


직원들은 배지를 사용해 엘리베이터를 타고 배정된 층으로 이동합니다.

직원은 다시 배지를 사용해 엘리베이터의 층 선택 기능을 활성화합니다.



원하는 층에 도착하면 직원의 사무 공간으로 걸어서 이동합니다.



ID 카드를 사용해 본인의 사무 공간에 들어갑니다.

직원이 본인의 책상에 앉으면 비밀번호를 사용해 컴퓨터의 잠금을 해제합니다.

제로 트러스트 원칙 활성화

엔드포인트 보안은 제로 트러스트 혁신의 핵심입니다.

제로 트러스트 전략을 효과적으로 구현하려면 엔드포인트를 보호해야 합니다.

MITRE ATT&CK® 프레임워크에 따르면 오늘날 공격자가 네트워크에 진입하기 위해 사용하는 9가지 '초기 액세스 기법'이 있습니다(그림 참조).[vi] 연구 결과에서 알 수 있듯이 클라우드 기반 환경에서는 기존의 방어 방식으로는 엔드포인트를 안전하게 보호할 수 없습니다. 공격자에게는 단 하나의 진입점만 있으면 됩니다. 위협 행위자는 엔드포인트를 통해 디바이스의 전체 수명주기에 걸쳐 수십 가지 취약성을 악용할 수 있습니다.

네트워크의 디바이스 수가 증가함에 따라 엔드포인트는 점점 더 큰 공격 벡터가 됩니다.

제로 트러스트 모델의 보안 정책은 '알려진 정상'을 명확하게 세부적으로 정의하고 다른 모든 것은 차단합니다. 그런 다음 위협 관리는 알려진 정상과의 편차를 모니터링하여 비정상적인 행동에 플래그를 지정하고 잠재적 위협을 해결하기 위한 적절한 조치를 트리거합니다.

그림 1/3

제로 트러스트 원칙 활성화

엔드포인트 보안은 제로 트러스트 혁신의 핵심입니다.

제로 트러스트 전략을 효과적으로 구현하려면 엔드포인트를 보호해야 합니다.

MITRE ATT&CK® 프레임워크에 따르면 오늘날 공격자가 네트워크에 진입하기 위해 사용하는 9가지 '초기 액세스 기법'이 있습니다(그림 참조).[vi] 연구 결과에서 알 수 있듯이 클라우드 기반 환경에서는 기존의 방어 방식으로는 엔드포인트를 안전하게 보호할 수 없습니다. 공격자에게는 단 하나의 진입점만 있으면 됩니다. 위협 행위자는 엔드포인트를 통해 디바이스의 전체 수명주기에 걸쳐 수십 가지 취약성을 악용할 수 있습니다.

네트워크의 디바이스 수가 증가함에 따라 엔드포인트는 점점 더 큰 공격 벡터가 됩니다.

제로 트러스트 모델의 보안 정책은 '알려진 정상'을 명확하게 세부적으로 정의하고 다른 모든 것은 차단합니다. 그런 다음 위협 관리는 알려진 정상과의 편차를 모니터링하여 비정상적인 행동에 플래그를 지정하고 잠재적 위협을 해결하기 위한 적절한 조치를 트리거합니다.

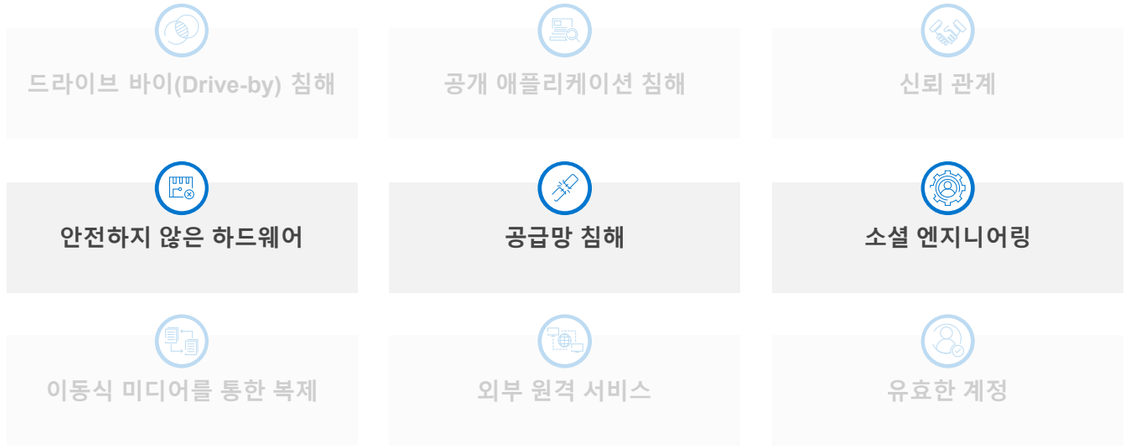


그림 2/3

제로 트러스트 원칙 활성화

엔드포인트 보안은 제로 트러스트 혁신의 핵심입니다.

제로 트러스트 전략을 효과적으로 구현하려면 엔드포인트를 보호해야 합니다.

MITRE ATT&CK® 프레임워크에 따르면 오늘날 공격자가 네트워크에 진입하기 위해 사용하는 9가지 '초기 액세스 기법'이 있습니다(그림 참조).[vi] 연구 결과에서 알 수 있듯이 클라우드 기반 환경에서는 기존의 방어 방식으로는 엔드포인트를 안전하게 보호할 수 없습니다. 공격자에게는 단 하나의 진입점만 있으면 됩니다. 위협 행위자는 엔드포인트를 통해 디바이스의 전체 수명주기에 걸쳐 수십 가지 취약성을 악용할 수 있습니다.

네트워크의 디바이스 수가 증가함에 따라 엔드포인트는 점점 더 큰 공격 벡터가 됩니다.

제로 트러스트 모델의 보안 정책은 '알려진 정상'을 명확하게 세부적으로 정의하고 다른 모든 것은 차단합니다. 그런 다음 위협 관리는 알려진 정상과의 편차를 모니터링하여 비정상적인 행동에 플래그를 지정하고 잠재적 위협을 해결하기 위한 적절한 조치를 트리거합니다.

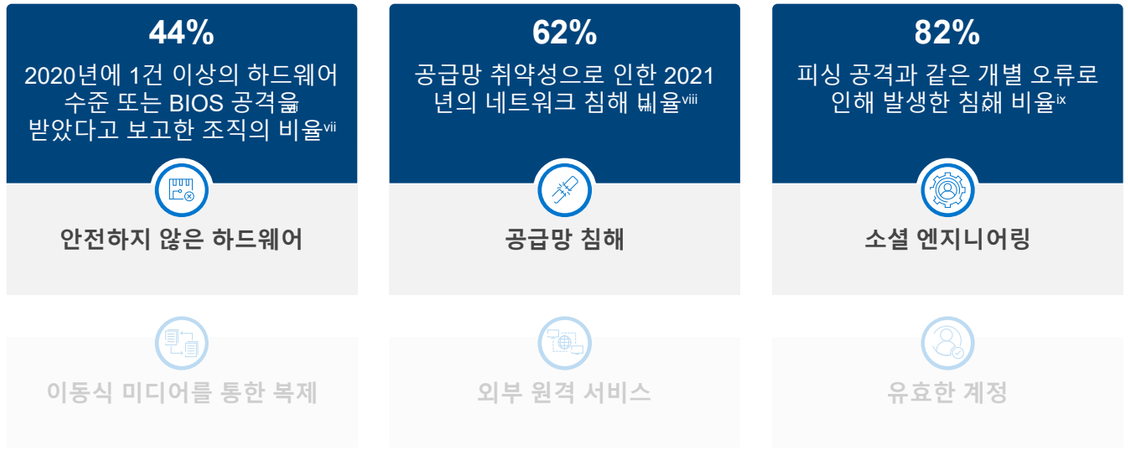


그림 3/3

제로 트러스트 준비를 위한 세 가지 권장 사항

성공적인 제로 트러스트 혁신을 위해 조직을 포지셔닝합니다.

1

비즈니스 우선 순위를 지원하는 적절한 정책 및 제어 기능을 마련합니다.

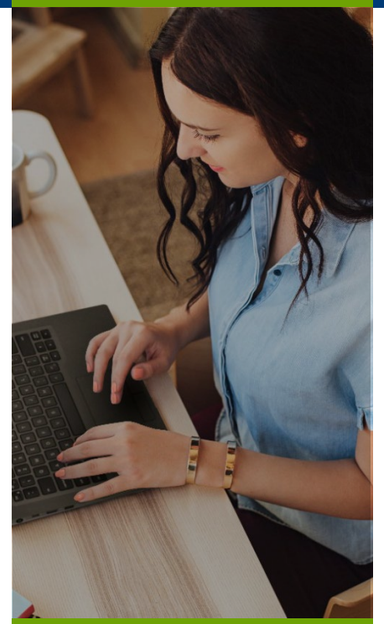
정책 엔진과 정책 관리는 효과적인 제로 트러스트 구현에 매우 중요합니다. 그러나 보안 예산이 무제한인 조직은 없으므로 먼저 비즈니스 우선 순위를 결정해야 합니다. 조직에서 보호하려는 가장 중요한 자산과 IP는 무엇입니까? 조직의 허용 가능한 위험과 공격 지점을 비교하십시오.

그런 다음 현재 시행 중인 정책 및 제어 기능을 검토합니다. 오늘날 위험은 우리가 생활하는 클라우드 기반 환경에서 비롯됩니다. 조직의 정책 엔진이 이를 고려하고 있습니까?

가장 중요한 자산에 대한 액세스를 제어하는 정책을 마련하면 적용 범위를 넓힐 수 있습니다.

자세한 정보

자세한 내용을 알아보려면 이 비디오를 시청하십시오. Dell Technologies의 사이버 전문가가 오늘날 조직이 직면한 주요 보안 위험을 설명합니다.



회사 네트워크 외부에 존재하는 사용자, 앱, 데이터 및 디바이스의 수가 그 어느 때보다 더 많아짐에 따라, IT 보안 의사 결정권자의 **82%**는 보안 정책을 재평가해야 했다고 말합니다.[x]

제로 트러스트 준비를 위한 세 가지 권장 사항

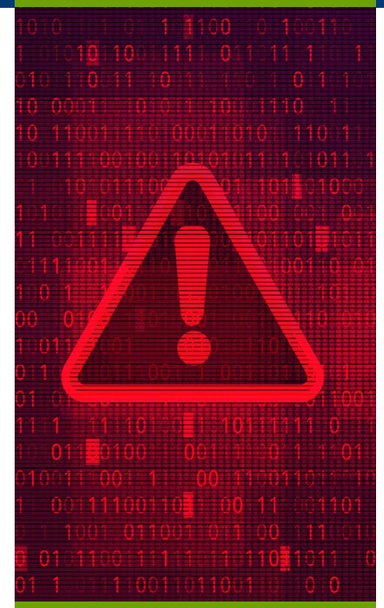
성공적인 제로 트러스트 혁신을 위해 조직을 포지셔닝합니다.

2 안전한 디바이스로 시작합니다.

제로 트러스트를 견고한 토대에 기반을 두고 계획합니다. 보안을 염두에 두고 설계 및 개발된 디바이스로 방어를 강화하십시오. 여기에는 다음이 포함됩니다.

A. **하드웨어 및 펌웨어 기반 보호**로 엔드포인트 스택을 보호하고 가시성을 확보합니다(예: BIOS가 손상되었는지 감지하고 IT에 경고). 직원 생산성에 미치는 영향을 가능한 한 최소화하면서 모든 새로운 액세스 요청에 대해 ID를 확인하는 기술을 조직에 제공합니다.

B. **공급망 보호 및 무결성 제어**로 PC 수명주기의 모든 단계를 보호합니다. 최근 몇 년간 살펴보았듯이 공급망 공격은 치명적일 수 있습니다. 진정한 제로 트러스트 아키텍처에서는 인증, 검증, 모니터링이 공급망에서 시작됩니다. 1) 보안 관행을 사용하고 2) 구매에서 제조, 배송에 이르기까지 디바이스의 무결성을 검증할 수 있는 공급업체와 협력하십시오.



2021년, 한 IT 관리 회사는 최소 **1,500**명의 고객에게 랜섬웨어 공격을 퍼뜨렸습니다.[xi]

자세한 정보

디바이스 보안의 모범 사례에 대한 자세한 내용은 Dell Technologies와 인텔의 백서인 Achieving Pervasive Security Above and Below the OS를 참조하시기 바랍니다.

제로 트러스트 준비를 위한 세 가지 권장 사항

성공적인 제로 트러스트 혁신을 위해 조직을 포지셔닝합니다.

3

생태계 전반에 걸쳐 원활한 통합 및 상호 운용성을 실현합니다.

효과적인 보안 태세를 갖추기 위해서는 다음 세 가지를 높은 수준으로 달성하는 것이 중요합니다.

A. IT 생태계 전반에 걸친 모든 방어 체계의 통합

B. 실시간 가시성

C. 필요할 때 조치를 취하는 역량

클라우드 기반 환경에서는 가장 작은 취약성이라도 방치할 경우 끔찍한 결과를 초래할 수 있으므로 모든 시스템이 잠재적 위협을 인식하고 동시에 필요한 조치를 취하도록 설정하는 것이 중요합니다.

시스템이 통합되어 있습니까 아니면 사일로에서 운영됩니까? IT 관리자가 네트워크의 손상된 BIOS에 대해 경고를 받는 경우 정책 엔진이 특정 워크플로를 트리거할 수 있습니까? 통합 환경에서 자동화는 문제가 되는 모든 BIOS를 즉시 격리하고 추가 액세스를 제한하며 패치 작업을 실행해야 합니다.

모든 엔드포인트에 대한 가시성이 있습니까? 이상적인 경우 공급망(예: 로딩 도크)에서 펌웨어(예: BIOS 수준 변조 경고)에 이르기까지 모든 계층에서 풍부한 텔레메트리 분석이 이뤄집니다.

그러나 텔레메트리 역량의 수준은 시스템 통합 수준에 따라 결정됩니다. 데이터를 처리할 수 있습니까? 문제를 해결하는 데이터 및 프로그램 워크플로를 이해하기 위해 적절한 리소스(예: 숙련된 사이버 보안 인재)를 확보하는 것이 중요합니다.

조직의 41%가 제로 트러스트를 배포하고 있습니다.[xii]

DELL Technologies

핵심 요점

보안의 미래는 제로 트러스트에 있습니다.

- 미래의 업무 방식을 받아들임에 따라 공격 벡터가 증가했습니다.
- 침해는 불가피해졌습니다. 최악의 시나리오에 대비하는 방어로 공격 지점을 최소화해야 합니다.
- 제로 트러스트는 보안에 관한 새로운 사고 방식으로, 조직이 IT 환경을 명시적으로 제어할 수 있게 합니다.
- 제로 트러스트 원칙을 활성화하는 엔드포인트 보호는 안전하고 현대적인 기반을 유지하는 데 핵심적입니다.
- 가장 중요한 자산을 정확히 파악하여 제로 트러스트 아키텍처 구축의 우선순위를 정해야 합니다.
- 기본 제공 보호 기능을 지원하고 공급망 제어에 철저하게 투자하는 공급업체의 디바이스를 공급받도록 합니다.
- 보안 및 IT 상호 운용성을 진단합니다. 계속해서 워크플로를 내장하여 보안 태세를 강화합니다.

다음 단계

보안은 어떤 규모의 조직이든 어려운 주제입니다. 경험이 풍부한 보안 및 기술 파트너와 협력하여 제로 트러스트 혁신을 간소화하십시오.

Dell Trusted Workspace는 최신 제로 트러스트 지원 IT 환경을 위한 엔드포인트 보안을 지원합니다. Dell만의 포괄적인 하드웨어 및 소프트웨어 보호 포트폴리오로 공격 지점을 줄이십시오. 고도로 조율된 방어 기반 접근 방식은 기본 제공 보호 기능과 지속적인 경계를 결합하여 위협을 상쇄합니다. 사용자는 생산성을 유지하고 IT 담당자는 오늘날의 클라우드 기반 환경을 위해 구축된 보안 솔루션으로 자신감을 유지할 수 있습니다.

문의처: EndpointSecurity@Dell.com

자세한 정보: Dell.com/Endpoint-Security

팔로우: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022년 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022년 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021년 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022년 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022년 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum, Four Keys to Navigating the Hardware Security Journey, 2020년 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon Data Breach Investigations Report, 2022년 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022년 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021년 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021년 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022년 https://www.ibm.com/security/data-breach