DELL Technologies

제로 트러스트
사이버 보안 향상을 향한 과정

숙련된 기술 및 보안 파트너와 함께 제로 트러스트 여정을 시작하십시오.

사이버 보안 성숙도를 높이는 조직은 제로 트러스트(Zero Trust) 지원 기능을 통해 공격 노출 지점을 줄이고, 사이버 위협을 탐지 및 대응하며, 사이버 공격 복구 방식을 구현하는 방법을 파악할 수 있도록 실행 가능한 로드맵을 구축하고 있습니다.

갈수록 정교해지는 사이버 위협에 대처하기 위해 Dell Technologies는 솔루션에 내장된 보안 기능을 활용하고 파트너와 협력해 고객이 비즈니스 목표에 부합하는 제로 트러스트를 달성하도록 지원합니다.

제로 트러스트란?

네트워크를 성이라고 상상해 보십시오. 다리가 내려와 누군가가 성 안으로 들어가면 그 안에서 자유롭게 돌아다닐 수 있습니다. 이제 경계 기반 방어 보안 모델을 더욱 현대적이고 안전한 제로 트러스트 프레임워크로 업데이트해야 합니다.

제로 트러스트는 귀하가 구매하는 제품과 다른, 아키텍처 측면의 보안 접근 방식입니다. 리소스에 대한 액세스 권한을 부여하기 전에는 사용자나 그 무엇도 절대로 신뢰하지 않으며 적법한 비즈니스 사용인지를 항상 검증합니다. 즉, 사용자와 디바이스가 사용 권한이 있는 네트워크에 연결되어 있고 이전에 검증된 경우에도 기본적으로 신뢰하지 않습니다.

절대 신뢰하지 않고 항상 검증합니다.

안전한 IT 생태계를 위한 기본 원칙입니다.

NIST(National Institute of Standards and Technologies)의 정의에 따르면 제로 트러스트 프레임워크는 미국 DoD(Department of Defense)에서 채택되어 아키텍처에 내장되어 있습니다.

여기에는 모든 보안 영역에서 Dell Technologies의 기준이 되는 7가지의 상호 연계된 핵심 요소가 포함되어 있습니다. 이러한 핵심 요소가 결합되어 다각적인 통합 아키텍처를 제공하며, 이를 통해 조직의 데이터와 인프라스트럭처를 보호하는 포괄적인 보안 접근 방식을 확보할 수 있습니다.

그동안 제로 트러스트는 다양한 보안 기능을 통합하고 여러 보안 제공업체 간에 파편화된 옵션을 탐색하는 복잡성으로 인해 도입에 어려움을 겪었습니다.

NIST

U.S. Department of Defense

DELL Technologies

제로 트러스트 성숙도를 높이십시오.

혁신 여정의 어느 단계에 있든지 Dell Technologies는 유용한 솔루션을 갖추고 있습니다.

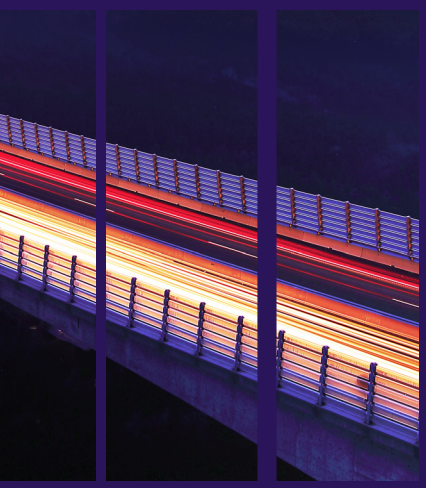
Dell Technologies는 조직에 선택권과 유연성을 제공합니다. 사이버 보안 성숙도를 높이고자 한다면, Dell Technologies는 악의적인 사이버 활동에 대비해 보강하고, 이러한 활동을 탐지 및 방어하며, 이로부터 복구하여 조직의 역량을 강화하는 제로 트러스트 기능을 갖춘 보안 솔루션을 제공할 수 있습니다.

제로 트러스트 원칙을 적용하십시오.

사이버 보안 성숙도를 높일 수 있는 선택권과 유연성을 제공합니다.

Dell Technologies는 보안 솔루션과 제로 트러스트 기능을 제공하여 악의적인 사이버 활동에 대비해 보강하고 이러한 활동을 탐지 및 방어하며 복구하는 역량을 강화합니다. 그 방법은 다음과 같습니다.

- 자동화, Threat Intelligence, 인증, 가시성 등을 강화하는 보호 기능 내장
- 제로 트러스트를 지원하기 위한 로드맵 개발, 주요 기술 통합 및 사전 예방적 관리 서비스
- 전문적인 매니지드 보안 자문 서비스
- 광범위한 파트너 생태계



제로 트러스트 도입을 획기적으로 간소화합니다.

완벽하게 통합된 아키텍처를 통해 전념할 수 있습니다.

제로 트러스트는 아키텍처 측면의 보안 접근 방식이기 때문에 단일 제품이 아니며 신중하게 계획된 솔루션이 조화를 이루어야 합니다. Dell Technologies는 제로 트러스트 통합 부담을 해소하고 있습니다. 그 방법은 다음과 같습니다.

- Dell Technologies는 미국 국방부에서 설계, 테스트 및 검증한 최초이자 유일한 완전 통합형 제로 트러스트 아키텍처를 구축하고 있습니다.

DELL Technologies

제로 트러스트 원칙을 적용하십시오.

특정 보안 생태계에 맞춰 구성한 방식으로 제로 트러스트를 달성합니다.

Dell Technologies는 제로 트러스트 전략을 지원함으로써 사이버 보안 성숙도를 높여 공격 노출 지점을 줄이고 탐지 역량을 강화하며 사이버 위협으로부터 신속하게 복구할 수 있도록 지원합니다.

그림으로 표현된 각 제로 트러스트 핵심 요소는 조직 보호를 위해 보안 및 비즈니스 정책이 필요한 핵심 영역에 부합하는 기술, 프로세스 및 인력을 설명합니다. Dell Security Services는 다음을 지원합니다.

- 보안 성숙도, 제로 트러스트, 위험 진단
- 전략과 로드맵 개발
- 핵심 제로 트러스트 기능의 매니지드 서비스

DELL Technologies

제로 트러스트의 기본 원칙

Dell Technologies는 제로 트러스트로 향하는 과정에 도움이 되는 고급 내장형 보안 솔루션을 제공합니다.

Dell Data Protection

Cyber Recovery 볼트 | PowerProtect Data Manager | CyberSense Transparent Snapshot | Cloud IQ | System Lockdown | 추이 탐지 | SEKM(Secure Enterprise Key Management) | TLS 1.3 | IPv6 | 다단계 인증 | SSO(Single Sign-On) | 역할 기반 액세스 | Cloud IQ

Dell PowerEdge 서버

SBOM(Software Bill of Materials) | 보안 구성 요소 검증 | 실리콘 RoT(Root of Trust) | System Lockdown | 추이 탐지 | SEKM(Secure Enterprise Key Management) | TLS 1.3 | IPv6 | 다단계 인증 | SSO(Single Sign-On) | 역할 기반 액세스 | Cloud IQ

Dell 스토리지 플랫폼

데이터 격리 | 데이터 불변성 | 위협 탐지 | 액세스 제어 인증 | 데이터 암호화 | STIG 강화 | 하드웨어 RoT(Root of Trust) | 보안 부팅 | 디지털 서명된 펌웨어 | 역할 기반 액세스 | 보안 스냅샷

Dell HCI/CI

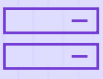
하드웨어 RoT(Root of Trust) | 보안 부팅 신뢰 체인 | 디지털 서명된 업데이트 | 키 관리 | 보안 로깅 | 분산 가상 스위치 | VM 격리 | 인증 및 권한 부여 | 생태계 커넥터 | 지속적으로 검증된 상태 | 소프트웨어 코드 무결성 | 전자 호환성 매트릭스

Dell PC

BIOS/펌웨어 보안 | 하드웨어 보안 | 공급망 보증 | 위협 관리 소프트웨어(EDR, XDR, VDR) | 네트워크 및 클라우드 데이터 보호 소프트웨어

Dell 엣지 솔루션

HW/SW/VM 증명 | 보안 온보딩 | 신뢰 체인 | 보안 OS/애플리케이션 제공 | 데이터 권한 관리



Dell 네트워크 스위치

SmartFabric | Cloud IQ | SD-WAN | VLAN 세분화 | Enterprise SONiC | ACL(Access Control List) | RADIUS | TACACS+ | 암호화 | 스위치 강화 | 마이크로 세분화 | 가상 라우팅 및 포워딩

DELL Technologies

Dell Technologies의 가속된 접근 방식.

빠르고 철저한 Project Fort Zero는 조직 전반에서 제로 트러스트를 전체적으로 통합합니다.

Project Fort Zero는 제로 트러스트 성숙도의 신속한 발전을 위한 검증된 방법을 제공하여 도입 시간을 단축하고 운영 중단을 줄이며 비용을 관리합니다.

미국 국방부에서는 업계 내 전문 지식과 영향력을 바탕으로 Dell Technologies에 제로 트러스트 도입 속도를 앞당길 수 있도록 지원해 달라고 요청했습니다. Dell Technologies는 민간 및 공공 부문 조직이 도입을 간소화하고 제로 트러스트 아키텍처를 전 세계적으로 확장하도록 지원하기 위해 생태계를 구축하고 30개 이상의 선도적인 기술 및 보안 회사의 통합을 주도하고 있습니다. Dell Technologies는 전 세계 민간 조직과 공공 기관 모두를 위한 제로 트러스트 아키텍처의 개발 및 글로벌 확장을 주도하고 있습니다. 이러한 활동에는 제로 트러스트를 달성하기 위한 미국 DoD의 목표를 향한 Dell Technologies의 의지가 잘 드러나 있습니다.

온프레미스

데이터 보안과 규정 준수가 가장 중요한 조직을 위한 데이터 센터.

원격 또는 지역

고객 데이터에 대한 안전한 실시간 분석을 통해 경쟁 우위를 확보할 수 있는 소매점과 같은 위치.

분리형 엣지

운영 연속성을 위해 일시적인 구현이 필요한 간헐적인 연결이 제공되는 비행기 또는 차량과 같은 장소.

DELL Technologies

Dell Technologies는 향상된 제로 트러스트를 위해 미국 DoD가 제시한 152개 활동을 모두 배포하여 제로 트러스트 도입을 가속할 수 있도록 지원합니다.

실행을 지원하는 요소

원칙 | 조직 | 교육 | 자료 | 리더십 및 교육 | 인력 | 시설 | 정책

제로 트러스트 타겟 수준

사용자 신뢰

- 사용자 인벤토리
- 앱 기반 사용 권한
- 규칙 기반 동적 액세스 1부
- 조직 MFA/IDP
- 시스템 구현 및 권한 있는 사용자 완화 1부
- 조직 ID 수명주기 관리
- 기본 정책에 따른 사용자 거부
- 단일 인증
- 시스템 구현 및 권한 있는 사용자 완화 2부
- 엔터프라이즈 ID 수명주기 관리 1부
- UEBA 툴링 구현
- 주기적 인증
- 엔터프라이즈 PKI/IDP 1부

디바이스 신뢰

- 디바이스 지원 툴 격차 분석
- NextGen AV 툴을 C2C와 통합
- 관리 중인 NPE/PKI 디바이스
- 기본 정책에 따른 디바이스 거부
- UEDM 또는 이에 상응하는 툴 구현
- 엔터프라이즈 디바이스 관리 1부
- EDR 툴 구현 및 C2C와 통합
- 자산, 취약성 및 패치 관리 툴 구현
- 엔터프라이즈 IDP 1부
- C2C/규정 준수 기반 네트워크 권한 부여 구현 1부
- 앱 제어 및 FIM 툴 구현
- 매니지드 및 제한적 BYOD 및 IOT 지원
- 엔터프라이즈 디바이스 관리 2부
- XDR 툴 구현 및 C2C와 통합 1부

애플리케이션과 워크로드

- 애플리케이션/코드 식별
- 리소스 권한 부여 1부
- DevSecOps 소프트웨어 팩토리 구축 1부
- 승인된 바이너리/코드
- 취약성 관리 프로그램 1부
- SDC 리소스 권한 부여 1부
- 리소스 권한 부여 2부
- DevSecOps 소프트웨어 팩토리 구축 2부
- 애플리케이션 보안 및 코드 문제 해결 자동화 1부
- 취약성 관리 프로그램 2부
- 지속적인 검증
- SDC 리소스 권한 부여 2부

데이터 신뢰

- 데이터 분석
- DLP 시행 지점 로깅 및 분석
- DRM 시행 지점 로깅 및 분석
- 데이터 태그 지정 표준 정의
- 데이터 태그 지정 및 분류 툴 구현
- 파일 활동 모니터링 1부
- DRM 및 보호 툴 구현 1부
- 시행 지점 구현
- 상호 운용성 표준
- SDS 정책 개발
- 수동 데이터 태그 지정 1부
- 파일 활동 모니터링 2부
- DRM 및 보호 툴 구현 2부
- 데이터 태그 및 분석을 통한 DLP 시행 1부
- DAAS 액세스와 SDS 정책 통합 1부
- 데이터 태그 및 분석을 통한 DRM 시행 1부
- SDS 솔루션 및 정책과 엔터프라이즈 IDP 통합 1부

네트워크와 환경

- 세분화된 제어 액세스 규칙 및 정책 정의 1부
- SDN API 정의
- 세분화된 제어 액세스 규칙 및 정책 정의 2부
- SDN 프로그래밍 가능 인프라스트럭처 구현
- 데이터 센터 매크로 세분화
- 마이크로 세분화 구현
- 제어 관리 및 데이터 플레인으로의 세그먼트 흐름
- B/C/P/S 매크로 세분화
- 애플리케이션 및 디바이스 마이크로 세분화
- 전송 중인 데이터 보호

자동화와 오케스트레이션

- 정책 인벤토리 및 개발
- 작업 자동화 분석
- 대응 자동화 분석
- 툴 규정 준수 분석
- 조직 액세스 프로파일
- SOAR 툴 구현
- 표준화된 API 호출 및 스키마 1부
- 워크플로 강화 1부
- 엔터프라이즈 보안 프로파일 1부
- 엔터프라이즈 통합 및 워크플로 프로비저닝 1부
- 데이터 태그 지정 및 분류 ML 툴 구현
- 표준화된 API 호출 및 스키마 2부
- 워크플로 강화 2부

가시성과 분석

- 확장 고려 사항
- 로그 파싱
- 자산 ID 및 알림 상관관계
- 위협 알림 1부
- 분석 툴 구현
- 사이버 Threat Intelligence 프로그램 1부
- 로그 분석
- 위협 알림 2부
- 사용자/디바이스 기준
- 사용자 기준 행동 설정
- 기준 및 프로파일링 1부
- 사이버 Threat Intelligence 프로그램 2부

총 타겟 활동 수: 91

출처: DoD Zero Trust Strategy Publication, 2022년 11월 7일

DELL Technologies

향상된 제로 트러스트

사용자 신뢰

- 규칙 기반 동적 액세스 2부
- 엔터프라이즈 역할 및 사용 권한 1부
- 유연한 대안 MFA 1부
- 실시간 승인 및 JIT/JEA 분석 1부
- 엔터프라이즈 ID 수명주기 관리 2부
- 사용자 활동 모니터링 1부
- 지속적인 인증 1부
- 지속적인 인증 2부
- 엔터프라이즈 PKI/IDP 3부
- 엔터프라이즈 역할 및 사용 권한 2부
- 유연한 대안 MFA 2부
- 실시간 승인 및 JIT/JEA 분석 2부
- 엔터프라이즈 ID 수명주기 관리 3부
- 사용자 활동 모니터링 2부
- 엔터프라이즈 PKI/IDP 2부

디바이스 신뢰

- 엔터프라이즈 IDP 2부
- C2C/규정 준수 기반 네트워크 권한 부여 구현 2부
- 엔터티 활동 모니터링 1부
- 디바이스 보안 슬랙과 C2C의 완전 통합
- 엔터프라이즈 PKI 1부
- 매니지드 및 완전한 BYOD 및 IOT 지원 1부
- XDR 툴 구현 및 C2C와 통합 2부
- 엔터티 활동 모니터링 2부
- 엔터프라이즈 PKI 2부
- 매니지드 및 완전한 BYOD 및 IOT 지원 2부

애플리케이션과 워크로드

- 리소스 권한 부여를 위한 속성 보강 1부
- 리소스 권한 부여를 위한 속성 보강 2부
- 지속적인 ATO(Authorization to Operate) 1부
- 애플리케이션 보안 및 코드 문제 해결 자동화 2부
- REST API 마이크로세그먼트
- 지속적인 ATO(Authorization to Operate) 2부

데이터 신뢰

- 수동 데이터 태그 지정 2부
- 데이터베이스 활동 모니터링
- 자동화된 데이터 태그 지정 및 지원 1부
- 데이터 태그 및 분석을 통한 DRM 시행 2부
- 데이터 태그 및 분석을 통한 DLP 시행 2부
- DAAS 액세스와 SDS 정책 통합 2부
- SDS 솔루션 및 정책과 엔터프라이즈 IDP 통합 2부
- SOS 툴 통합 및/또는 DRM 툴과 통합 1부
- 자동화된 데이터 태그 지정 및 지원 2부
- 포괄적인 데이터 활동 모니터링
- 데이터 태그 및 분석을 통한 DRM 시행 3부
- 데이터 태그 및 분석을 통한 DLP 시행 3부
- DAAS 액세스와 SDS 정책 통합 3부
- SDS 툴 통합 및/또는 DRM 툴과 통합 2부

네트워크와 환경

- 네트워크 자산 검색 및 최적화
- 실시간 액세스 결정
- 마이크로 세분화 처리

자동화와 오케스트레이션

- 엔터프라이즈 보안 프로파일 2부
- 엔터프라이즈 통합 및 워크플로 프로비저닝 2부
- AI 자동화 툴 구현
- 워크플로 강화 3부
- 분석 기반 AI에서 A&O 수정 결정
- 플레이북 구현
- 자동화된 워크플로

가시성과 분석

- 위협 알림 3부
- 기준 및 프로파일링 2부
- UEBA 기준 지원 1부
- UEBA 기준 지원 2부
- AI 지원 네트워크 액세스
- AI 지원 동적 액세스 제어

총 고급 활동 수: 61

Dell Technologies는 제로 트러스트 성숙도를 빠르게 달성할 수 있도록 복잡성을 단순화할 수 있습니다.

출처: DoD Zero Trust Strategy Publication, 2022년 11월 7일

DELL Technologies

모든 조직의 요구를 충족합니다.

제로 트러스트 성숙도를 높이십시오.

제로 트러스트는 보안 접근법과 다양한 기능을 사용하여 구현할 수 있는 방법을 안내하는 정의된 프레임워크이자 일련의 원칙입니다. 제로 트러스트에 전념하든, 타겟 개선에 집중하든, Dell Technologies는 제로 트러스트 원칙에 맞춰 보안 여정을 발전시키는 데 도움을 주는 숙련된 보안 파트너입니다.

화학

정보 기술

커뮤니케이션

응급 서비스

식품과 농업

방위

의료와 공중 보건

제조

금융

핵 원자로

커머셜

정부

에너지

운송

물과 폐수

댐

DELL Technologies

DELL Technologies

귀사의 제로 트러스트 여정을 위한 숙련된 기술 및 보안 파트너입니다.

제로 트러스트를 구현하여 장기적으로 사이버 보안을 개선합니다.

Dell Security Services의 오퍼링

보안 성숙도 및 전반적인 위험에 대한 전문가 진단

제로 트러스트 로드맵 개발

지속적인 보안 활동 관리

DELL Technologies

Dell.com/SecuritySolutions

콜백 요청

보안 어드바이저와 채팅 상담

전화 1-800-433-2393