DELL Technologies

사이버 보안 및 회복탄력성 성숙도 강화

사이버 보안 성숙도는 모든 현대 비즈니스의 전략적 핵심 요소

오늘날의 사이버 위협 환경은 그 어느 때보다 역동적이고 가혹하며, AI 기반 공격은 빈도, 속도, 정교함 면에서 점점 더 증가하고 있습니다. 조직은 더 이상 임시방편적인 방어나 점진적인 업데이트에만 의존할 수 없습니다.

비즈니스 리더는 데이터 침해가 임박하지 않았더라도 불가피하다고 생각하고 기업을 운영해야 합니다. Dell Technologies는 고객이 사이버 위험에 직면하여 비즈니스를 운영하는 데 있어 갖는 자신감 수준인 보안 성숙도를 높일 수 있도록 지원합니다. 이를 위해 세 가지 핵심 실행 영역을 중심으로 구축된 포괄적이고 다층적인 사이버 보안 및 회복탄력성 접근 방식을 발전시켜 나갑니다.

기업은 다음과 같은 역량을 갖춰야 합니다.

- **공격 노출 지점 축소**
- **사이버 위협 탐지 및 대응**
- **사이버 공격으로부터 복구**

효과적인 사이버 보안은 현재의 보안 태세와 성숙도를 솔직하게 평가하는 것에서 시작됩니다. 이처럼 명확한 평가를 통해 적절한 개선 사항의 우선순위를 정하고 더욱 안전한 미래를 위한 투자를 할 수 있습니다.

공격 노출 지점 축소

조직의 공격 노출 지점은 역동적이며 빠르게 진화하고 있습니다. AI는 새로운 공격 벡터를 만들어내고 있으며, 원격 근무와 기존 시스템은 공격 노출 지점을 더욱 넓혀 위협 행위자가 침입할 수 있는 지점을 늘립니다. 따라서 공격 노출 지점을 축소하는 것은 위험을 줄이고, 규정 준수 의무를 이행하고, 조직의 회복탄력성을 보호하고, 기본적인 신뢰도를 구축하는 데 있어 전략적으로 필수적입니다.

사이버 보안 및 회복탄력성 성숙도 강화

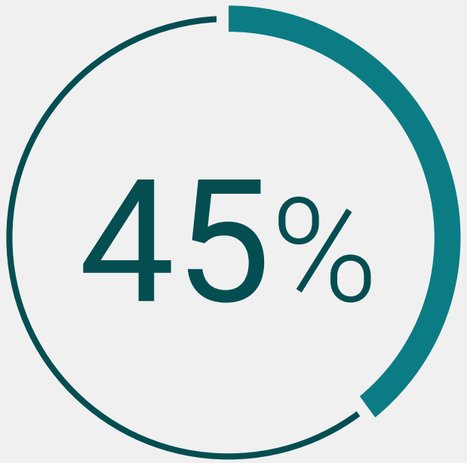
공격 노출 지점을 축소하면 공격자가 악용할 수 있는 진입점을 최소화하여 전반적인 위험을 낮출 수 있습니다. 이는 보안 성숙도를 강화하고 규정 준수 노력을 간소화합니다. 결과적으로 회복탄력성이 강화되고, 인시던트를 예방하여 비용을 절감하고, 보안이 처음부터 내재되어 있다는 확신을 가지고 더 빠르게 움직이고, 더 자유롭게 혁신하고, 새로운 시장에 진출할 수 있습니다. 이는 제로 트러스트 원칙(절대 신뢰하지 말고 항상 검증)을 채택하고 사용자, 디바이스 및 애플리케이션 전반에 걸쳐 최소 권한 원칙을 적용하는 것에서 시작됩니다.

Dell Technologies는 "보안 설계 내재화"라는 사고방식을 수용합니다. 사이버 보안은 안전한 글로벌 공급망부터 핵심 제품에 내장된 보호 기능에 이르기까지 Dell Technologies의 모든 활동에 내재되어 있습니다. 이러한 보호 조치는 하드웨어 수준에서 시작하여 디바이스가 신뢰할 수 있는 소프트웨어만 시작하고 실행되도록 보장합니다. Dell Technologies는 제로 트러스트 원칙에 맞춰 솔루션을 제공함으로써 취약성을 공격자가 악용하기 전에 제거할 수 있도록 지원합니다. 예를 들어, 세계 최고 수준의 보안을 자랑하는 Dell Technologies의 AI PC [1]는 현대적인 작업 공간을 위한 기본적인 방어 체계를 제공합니다.

공격 노출 지점을 축소하면 불확실성이 제거되어 보안 성숙도가 향상됩니다. 즉, 알려지지 않은 요소, 진입점, 그리고 예상치 못한 상황이 줄어듭니다.

주요 고객 성과:

- **취약성 최소화:** 엔드포인트, 인프라스트럭처 및 애플리케이션을 사전 예방적으로 강화함으로써 공격자의 공격 기회를 크게 줄일 수 있습니다.
- **간소화된 보안 관리:** 노출된 자산이 줄어들면 관리해야 할 제어 항목이 줄어들어 더욱 효율적이고 간소화된 보안 태세를 구축할 수 있습니다.
- **혁신을 위한 더욱 강력한 기반:** 신뢰할 수 있는 엔드포인트와 보호된 데이터를 통해 AI 및 엣지 컴퓨팅과 같은 새로운 기술을 더욱 자신 있게 도입할 수 있습니다.



공격 노출 지점 축소에 집중하는 조직은 외부 노출 관리 시 사이버 침해 위험을 45% 줄일 수 있습니다.[2]

사이버 위협 탐지 및 대응

사이버 보안 분야에서는 속도와 인텔리전스가 불가분의 관계입니다. 효과적인 탐지 및 대응을 통해 위협을 신속하게 식별하고 차단하여 공격 체류 시간을 줄이고 공격으로 인한 피해를 최소화할 수 있습니다. 결과적으로 비용 절감, 다운타임 감소, 그리고 지속적인 위협 속에서도 비즈니스를 안전하게 운영할 수 있다는 운영 신뢰성을 높일 수 있습니다.

사이버 보안 및 회복탄력성 성숙도 강화

하지만 많은 조직은 하이브리드 환경에서 가시성이 부족하고, 엄청난 양의 알림에 시달리고 있습니다. 공격자는 이제 네트워크 내에서 평균 11일 동안 잠복한 후에야 발견됩니다. 이러한 문제를 해결하려면 지속적인 모니터링, Threat Intelligence, 자동화를 통해 엔드포인트, 네트워크 및 시스템 전반에 걸쳐 실시간 가시성을 확보해야 합니다.

올바른 보안 파트너는 Threat Intelligence 및 인시던트 대응 분야에서 전문적인 지식을 제공합니다. Dell은 고급 분석, AI/ML 기반 위협 탐지, 24x7 매니지드 서비스를 안전한 하드웨어 기반과 결합하여 운영 위협이 중단을 초래하기 전에 식별하고 차단합니다. MDR(Managed Detection and Response)과 같은 선택적 서비스는 보안 전문 지식을 제공하여 가시성을 확장하고 위협에 신속하게 대응하고 완화할 수 있도록 지원합니다.

강력한 탐지 및 대응 기능은 체류 시간을 단축하고 위협 발생 시 팀이 신속하게 대응할 수 있다는 확신을 심어줌으로써 보안 성숙도를 향상합니다.

주요 고객 성과:

- **더 빠른 탐지 및 체류 시간 단축:** MDR(Managed Detection and Response)은 탐지 및 대응에 소요되는 평균 시간을 25~49% 단축하여 공격이 더욱 심각해질 가능성을 줄입니다.
- **운영 부담 감소:** 전문가와의 협력을 통해 사전 예방적 위협 탐지 및 지속적인 모니터링을 수행함으로써 내부 팀의 부담을 줄이고 전략적인 업무에 집중할 수 있도록 지원합니다.
- **회복탄력성 향상:** 성숙한 탐지 및 대응 기능은 보안 인시던트 발생률을 낮추고 침해 관련 비용 증가를 방지하는 데 도움이 됩니다.

$4.44M

2025년에 데이터 침해로 인한 평균 비용은 444만 달러에 달했습니다.[3]

사이버 공격으로부터 복구

최악의 시나리오가 발생했을 때, 최우선 목표는 최소한의 중단으로 최대한 신속하게 정상 운영으로 복귀하는 것입니다. 사이버 공격으로부터 복구하면 깨끗한 데이터와 시스템을 신속하게 복원하여 평판 손상을 최소화하고, 복구가 안정적이며 재감염되지 않았다는 확신을 얻을 수 있습니다.

사이버 보안 및 회복탄력성 성숙도 강화

최강의 방어 체계를 구축하더라도 공격은 불가피하다고 가정하고 계획을 세워야 합니다. 완벽한 복구 계획과 역량을 갖추는 것이 매우 중요합니다. 여기에는 격리된 복구 볼트에 중요 데이터의 깨끗하고 변경 불가능한 백업을 유지하고, 클린룸 환경에서 복원된 시스템에 멀웨어가 없는지 검증한 후 시스템을 다시 온라인 상태로 전환하는 작업이 포함됩니다.

Dell Technologies는 제품 오퍼링에 복구 기능을 구축하며, 인시던트 발생 시 비즈니스를 정상 운영 상태로 되돌리는 것을 최우선 과제로 삼고 있습니다. PowerProtect Cyber Recovery 볼트와 같은 솔루션은 중요 데이터의 깨끗한 복사본을 격리하고 보호하여 신속한 복구를 지원함으로써 데이터 손실을 최소화하고 랜섬웨어 공격자의 압박을 줄여줍니다. 이러한 아키텍처를 통해 중요 워크로드를 신속하게 다시 온라인 상태로 전환하여 안심하고 운영할 수 있습니다.

복구 단계는 보안 성숙도의 실질적인 시험대가 됩니다. 비즈니스가 얼마나 신속하고 완전하게 정상 운영으로 돌아갈 수 있는지에 따라 조직의 신뢰도가 좌우되기 때문입니다.

주요 고객 성과:

- **비즈니스 영향 감소:** 잘 짜여진 인시던트 대응 계획을 갖춘 조직은 침해로 인한 비용을 약 61% 절감할 수 있습니다.
- **운영 재개 속도 향상:** 위협 제거뿐 아니라 신속한 비즈니스 복귀를 우선시함으로써 최소한의 중단과 비용으로 운영을 복원할 수 있습니다.
- **데이터 무결성 향상:** 중요 데이터를 격리하고, 변경 불가능한 복사본을 사용하며, 복원 전에 무결성을 검증함으로써 복구 프로세스에 대한 신뢰도를 높일 수 있습니다.

의 조직은 서비스 수준 계약을 준수하면서 사이버 공격으로부터 복구하는 데 어려움을 겪을 것이라고 인정했습니다.[4]

전략적 파트너십을 통해 보안 성숙도 강화

오늘날의 빠르게 변화하고 복잡한 사이버 보안 환경에서 성공하려면 경험이 풍부한 파트너가 필수적입니다. 사이버 위협은 더욱 정교해지고 빈번해짐에 따라 단일 조직이 앞서 나가는 데 필요한 전문 지식, 리소스 및 기술을 유지하는 것은 거의 불가능합니다. Dell Technologies와 같은 보안 리더와 협력함으로써 기업은 전문 기술, 첨단 기술 및 신뢰할 수 있는 파트너 네트워크를 활용할 수 있습니다. 이러한 파트너십은 위협을 효과적으로 탐지, 예방 및 대응하는 데 필요한 지원과 전문 지식을 제공하여 끊임없이 진화하는 디지털 환경에서 비즈니스를 안전하게 보호합니다.

이 세 가지 실행 영역에 걸쳐 올바른 접근 방식을 통해 조직은 보안 성숙도를 높여 지속적인 사이버 압력 속에서도 운영하고, 혁신하고, 성장할 수 있다는 자신감을 구축할 수 있습니다. Dell Technologies는 신뢰할 수 있는 인프라스트럭처, 신뢰할 수 있는 작업 공간, 고급 서비스 및 파트너 생태계를 결합하여 조직이 안전하고, 적응력이 뛰어나며, 회복탄력성을 유지하여 미래에 대비할 수 있도록 지원합니다.

보안 솔루션 둘러보기

DELL Technologies

자주 묻는 질문

1. 사이버 보안이 비즈니스의 최우선순위가 되어야 하는 이유는 무엇입니까?
사이버 보안은 단순한 보호 이상의 의미를 지닙니다. 위험한 사이버 보안 환경 속에서도 기업이 혁신하고 성장할 수 있도록 하는 기반입니다. 강력한 보안 태세는 단순한 방어가 아니라 기업의 성장을 가능하게 하는 것입니다. 성숙한 사이버 보안 프레임워크를 갖춘 기업은 더 빠르게 움직이고, 더 자유롭게 혁신하며, 자신감을 가지고 새로운 시장에 진출할 수 있습니다. 또한 규제 변화, 고객 요구, 경쟁 압력에 더 잘 대응할 수 있습니다.

2. 엄격한 보안 요구와 혁신의 자유 사이에서 어떻게 균형을 맞출 수 있습니까?
보안과 혁신 사이에서 선택할 필요는 없습니다. Dell Technologies는 강력한 보안이 오히려 혁신을 촉진한다고 생각합니다. 처음부터 디바이스, 인프라스트럭처 및 데이터에 보안이 내재된 "보안 설계 내재화" 기반을 갖추면 팀은 AI 및 엣지 컴퓨팅과 같은 새로운 기술을 자신 있게 도입할 수 있습니다.

3. 공급망 보안은 왜 그렇게 중요한 것입니까?
진정한 보안은 전원 버튼을 누르기 훨씬 전부터 시작됩니다. 디지털 범위가 커질수록 노출 위험도 커지기 때문에 신뢰가 최우선 방어선이 됩니다. 공급망의 모든 연결 고리를 보호해야 합니다. 단 하나의 구성 요소라도 손상되면 아무리 최첨단 소프트웨어라도 무용지물이 될 수 있기 때문입니다. 그래서 Dell Technologies는 생산부터 배포까지 모든 단계를 보호하는 보안 시스템을 처음부터 구축합니다. 공장에서 최종 사용자에게 이르기까지, 모든 기술은 신뢰할 수 있고 검증되었으며, 안정적인 성능을 제공하도록 설계되었습니다.

4. Dell Technologies는 사이버 공격 후 복구를 어떻게 지원합니까?
인시던트 발생 시 다운타임과 중단을 최소화하는 것이 중요합니다. 사전 준비가 핵심입니다. PowerProtect Cyber Recovery 볼트는 가장 중요한 데이터의 깨끗하고 변경 불가능한 복사본을 기본 환경과 안전하게 분리합니다. 인시던트 발생 시, 손상 없이 신속하고 안전하게 운영을 복원할 수 있으며, 대가를 지불할 필요도 없습니다.
Dell Technologies는 포괄적인 복구 전략을 구현하는 데 도움이 되도록 설계된 다양한 제품과 서비스를 제공합니다. 복구 및 교육 계획 수립을 위한 컨설팅 서비스부터 중요 데이터를 안전하게 보호할 수 있는 데이터 보호 기능에 이르기까지 다양한 서비스를 제공합니다. Dell Technologies는 사람과 기술 중심적인 접근 방식을 취해 직원과 기술이 협력하여 신속하게 복구할 수 있도록 지원합니다.

5. Dell Technologies에서 실시간 위협 탐지를 지원할 수 있습니까?
그렇습니다. 사이버 위협을 차단하는 데 있어 속도는 매우 중요합니다. Dell Technologies는 내장된 보안 기능과 MDR(Managed Detection and Response)과 같은 고급 서비스를 결합하여 연중무휴 24시간 모니터링합니다. AI/ML 기반 인사이트와 전문가의 도움을 받아 이상 징후와 잠재적 위협을 즉시 파악하여 비즈니스에 영향을 미치기 전에 문제를 해결하고 차단할 수 있도록 지원합니다.

출처

[1] Dell Technologies 내부 분석 기준, 2024년 10월(인텔) 및 2025년 3월(AMD). 인텔 및 AMD 프로세서를 탑재한 PC에 해당됩니다. 일부 기능을 지원하지 않는 PC도 있습니다. 일부 기능을 사용하려면 추가로 구매해야 합니다. Principled Technologies에서 검증한 인텔 기반 PC, 2025년 7월 신뢰할 수 있는 디바이스의 구조 인포그래픽

[2] Forrester Consulting, “The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight,” 2024년 10월.

[3] IBM 및 Ponemon Institute, “Cost of a Data Breach Report 2025: The AI Oversight Gap,” 2025.

[4] Dell Technologies, "사이버 보안 성숙도 향상: 모든 현대 비즈니스의 핵심 요소인 기술 인프라스트럭처", 2025년 2월.

Dell Technologies 소개

Dell Technologies(NYSE: DELL)는 조직 및 개인이 디지털 미래를 구축하고 업무 처리와 생활 방식은 물론 여가를 보내는 방식도 혁신하도록 돕고 있습니다. Dell Technologies는 AI 시대를 맞이하여 업계에서 가장 광범위하고 혁신적인 수준의 기술 및 서비스 포트폴리오를 제공합니다.

자세한 내용은 Dell.com을 참조하십시오.