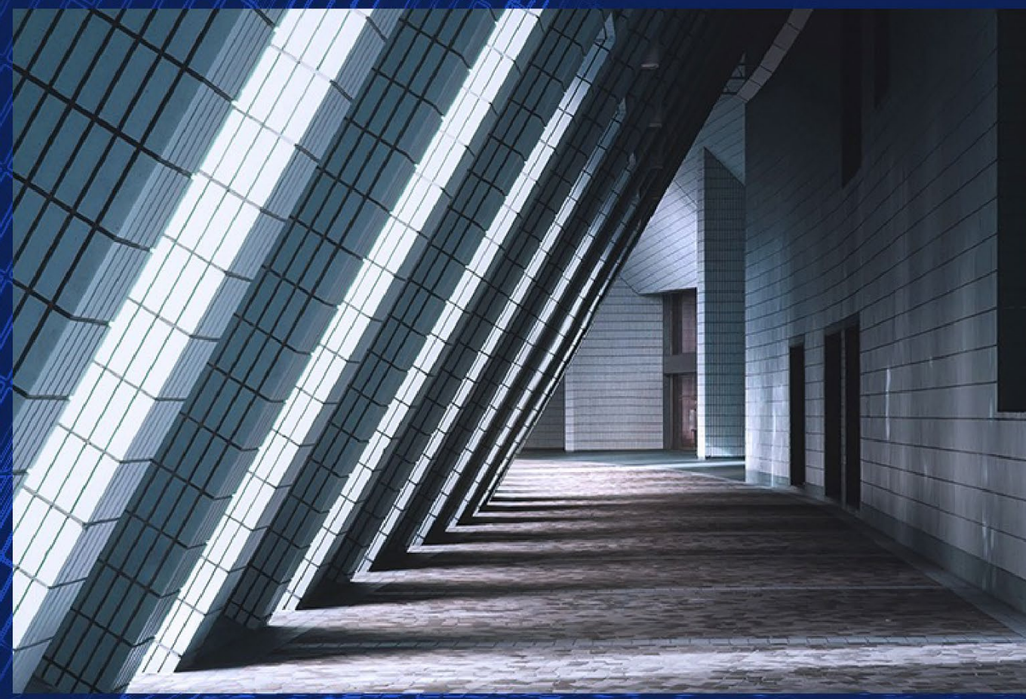
DELL Technologies



사이버 보안 역량 강화

모든 현대 비즈니스의 핵심 요소인 기술 인프라스트럭처

보안과 회복탄력성은 중요한 요소가 작동하는 데 유의미한 역할을 합니다. 그러나 많은 기업이 진화하는 위협에 대응하는 데 어려움을 겪고 있습니다. 실제로 최근 연구에 따르면 조직의 93%가 보안 전략을 개선해야 한다고 인정합니다.

문제는 조직이 사이버 위협에 직면할 것인지가 아니라 언제 어떻게 직면할 것인가입니다. 비즈니스 리더는 데이터 침해가 임박하지 않았더라도 불가피하다고 생각하고 기업을 운영해야 합니다. 동시에 보안 위험이 조직의 혁신 능력을 저해하지 않도록 해야 합니다. 연구 결과에 따르면 응답자의 79%가 보안과 혁신의 균형을 맞추는 데 어려움을 겪고 있습니다.

점점 더 정교해지는 사이버 위협과 AI(Artificial Intelligence)와 같은 기술의 급속한 확산으로 인해 사전 예방적 보안 사고방식이 그 어느 때보다 필수적입니다. 앞으로 나아갈 길은 세 가지 중요한 보안 중점 영역으로 구성됩니다. 기업은 다음과 같은 강력한 역량을 갖춰야 합니다.

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

공격 노출 지점 줄이기

조직의 공격 노출 지점은 매우 동적이며 빠르게 진화하고 있습니다. 지난 10년 동안 조직의 공격 노출 지점이 약 1,000% 증가했으며, 이는 모던 디지털 환경의 보안 복잡성이 증가하고 있음을 반영합니다.

각각의 새로운 기술 발전은 잠재적인 보안 격차를 야기합니다. 예를 들어 GenAI(Generative AI)는 데이터 노출, 결과 조작, 기밀 정보 공개, 프롬프트 주입 등과 관련하여 새로운 위험을 초래합니다. AI 구현 이외의 영역에서도 보안 과제에 맞닥뜨리게 됩니다. 실제로 비즈니스 리더의 67%는 새로운 혁신이 공격 노출 지점을 증가시킬 것이라고 우려하고 있습니다.

공격 노출 지점을 줄이려면 다계층 접근 방식이 필요합니다. 보안 격차를 최대한 방지하기 위해 철저한 침투 테스트와 취약성 진단을 포함하여 기본적인 관행으로부터 시작하여 즉각적인 주의가 필요한 잠재적인 보안 격차를 파악하고 해결합니다. 아울러 포괄적인 네트워크 세분화, 중요 데이터 격리, 엄격한 액세스 제어 적용, 시스템과 애플리케이션의 정기 업데이트 및 패치 적용 등은 필수입니다.

또한 사이버 보안은 지속적인 프로세스이며 유한한 활동이 아니므로 조직과 위협 환경이 지속적으로 진화하고 있으므로 초기 침투 테스트 및 취약성 평가를 정기적으로 수행해야 합니다.

Dell Technologies는 "보안 기능 내장"이라는 개념을 지지합니다. 이는 안전한 공급망에서 출발하며 Dell Technologies의 핵심 제품에 포함되어 있는 MFA(Multi-Factor Authentication)를 통한 ID 액세스 관리 및 RBAC(Role-Based Access Control)와 같은 제로 트러스트 원칙을 포괄합니다. Dell Technologies는 이러한 기능들이 강력하게 작동하는, 가장 안전한 AI PC를 제공합니다.

85%

공급망이 보안 태세에 매우 중요하다는 데 동의하는 비즈니스 리더의 비율.

54% GenAI를 이미 구현 중이거나 향후 12개월 이내에 구현할 계획인 조직의 비율.

56% GenAI 위험에 대해 우려하고 있는 ITDM(IT Decision-Maker)의 비율.

32% GenAI가 보안을 강화할 잠재력이 있다고 생각하는 ITDM의 비율.

사이버 위협 탐지 및 대응

사이버 방어 분야에서는 속도와 인텔리전스가 서로 밀접하게 관련되어 있습니다. 기업은 보안 침해의 초기 단계에서 잠재적인 보안 인시던트 및 악의적인 활동을 적극적으로 식별하고 해결하기 위해 노력해야 합니다.

여기서 AI 및 머신 러닝 알고리듬을 기반으로 하는 위협 탐지 기술은 기본이 됩니다. 이러한 시스템은 AI를 사용하여 네트워크 트래픽, 데이터 패턴 및 사용자 행동을 실시간으로 모니터링하여 가능한 보안 위협을 정확히 찾아냅니다.

적절한 보안 파트너는 위협 인텔리전스 및 인시던트 대응에 대한 전문 지식을 제공할 수도 있습니다. Dell Technologies는 PC 및 인프라스트럭처 제품에 직접 보안을 구축합니다. MDR(Managed Detection and Response)과 같은 선택적 서비스는 위협을 식별하고 대응하는 데 도움이 됩니다.

80%

사이버 위협 탐지 및 대응 기능을 개선할 수 있다고 인정하는 조직의 비율.

사이버 공격으로부터 복구

최악의 시나리오가 발생하면 중단을 최소화하면서 가능한 한 빨리 정상 상태로 복귀하는 것을 기본 목표로 삼아야 합니다. 그러나 최근 조사에서는 64%의 조직이 SLA를 준수해야 하는 상황에서 사이버 공격으로부터 복구하는 데 어려움이 있을 것이라고 응답했습니다.

가장 강력한 방어 체계를 구축해야 하지만, 공격이 불가피하다는 가정으로 계획을 세워야 합니다. 따라서 복구 계획과 기능을 갖추는 것이 중요합니다. 여기에는 암호화를 활용하여 오프사이트 스토리지를 변경이 불가능하게 하거나 격리하거나 안전하게 유지함과 동시에 중요한 데이터와 시스템의 안전한 백업을 유지하는 것이 포함됩니다. 또한 공격이 발생하는 순간부터 모든 당사자의 역할과 책임을 요약하는 명확한 인시던트 대응 프로토콜을 수립하고 내부 팀과 파트너 간의 원활한 조정을 위한 채널을 식별하는 작업도 포함됩니다. 마지막으로, 준비 상태를 보장하기 위해 다양한 공격 시나리오를 시뮬레이션하는 등 복구 절차를 정기적으로 테스트해야 합니다.

Dell Tehcnologies는 제품 오퍼링에 복구 기능을 구축하며, 인시던트 발생 시 비즈니스를 정상으로 되돌리는 것을 최우선 과제로 삼고 있습니다. ASR(Automated System Recovery)을 지원하는 PowerEdge 서버, 변경 불가능한 스토리지에 대한 고급 스냅샷 기능을 갖춘 PowerStore 및 PowerMax 시스템, 그리고 PowerProtect Cyber Recovery 볼트와 같은 솔루션은 가장 중요한 데이터가 온전히 유지되도록 지원합니다.

65%

SLA를 준수해야 하는 상황에서 사이버 공격으로부터 복구하는 데 어려움이 있을 것이라고 인정한 조직의 비율.

전략적 파트너십을 통한 보안 태세 강화

사이버 보안과 회복탄력성의 성장을 위해서는 지속적인 경계와 발전을 추구해야 합니다. 강한 보안 및 재난 대응 태세를 유지하면 조직은 위험 노출을 크게 줄일 수 있습니다. 또한 재정적 손실을 최소화하고 운영 효율성을 개선하며 고객들과의 신뢰도를 높일 수 있습니다.

숙련된 파트너가 빠르게 변화하는 환경을 탐색하는 데 도움을 줄 수 있습니다. 기업들은 Dell Technologies와 같은 보안 선도 기업과 협업하여 새로운 위험에 대한 통찰력, 지능형 공격 기법, 최신 보안 전략 및 모범 사례 등 사내에서 제공할 수 없는 전문 기술과 지식을 제공 받고 있습니다.

기업은 공격 지점을 줄이고 위협을 탐지하고 이에 대응하며 인시던트로부터 복구하는 올바른 접근 방식을 통해 오늘날과 같은 디지털 시대에서 성공하는 데 필요한 회복탄력성을 구축할 수 있고 이를 기반으로 미래의 당면 과제를 해결하기 위한 혁신을 수행할 수 있습니다.

Dell Technologies의 보안 솔루션에 대해 자세히 알아보십시오.

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.

이 eBook의 모든 데이터 정보는 2025년 2월 미국, 영국, 독일, 프랑스, 일본의 모든 부문에 걸쳐 750명의 비즈니스 및 IT 의사 결정권자를 대상으로 실시한 Dell Technologies 설문조사에서 얻은 것입니다. 전체 결과는 여기에서 확인 가능합니다.