Microsoft

두 단계로 생산성을 안전하게 보호하는 방법에 대해 알아보기

제로 트러스트 기반을 통해 생산적인 업무 경험을 강화하는 방법

목차

소개

증가하는 위협 환경에 적응하지 말고 앞서 나가기

오늘날 위협 환경은 ID 공격, 랜섬웨어, 엔드포인트 공격과 같은 정교한 위협으로 인해 데이터 및 IT 인프라를 위험에 빠뜨리면서 빠르게 성장하고 있습니다. 현대적인 업무의 현실은 IT 팀에 대한 압박을 가중시키고 있으며, IT 팀은 점점 더 많은 취약점을 처리하느라 바쁜 시간을 보내고 있습니다.

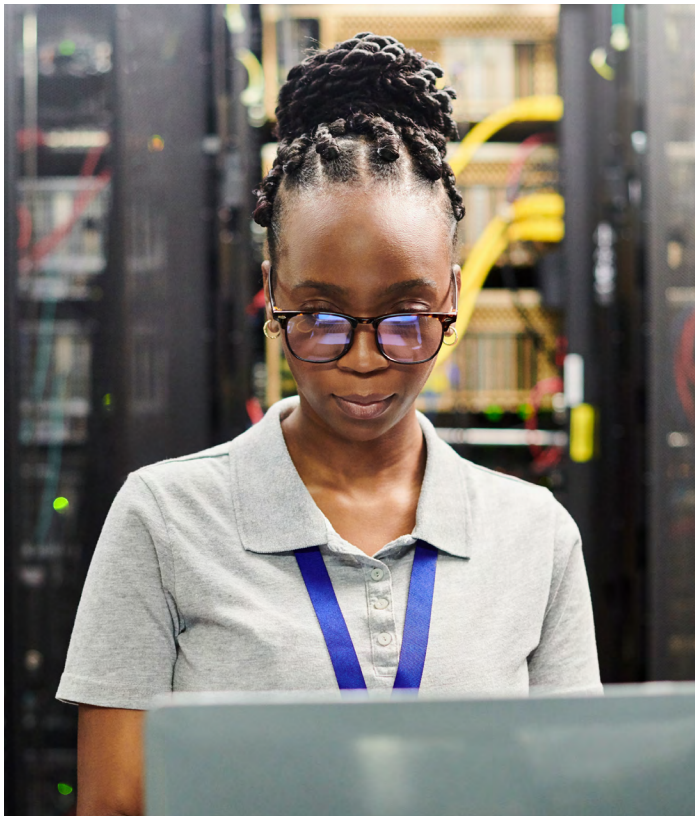
IT 전문가 중 **67%**가 원격 근무를 관리하는 데 어려움을 겪고 있다고 보고한 가운데, 비용이 많이 드는 침해 및 다운타임을 방지하기 위해서는 위협에 미리 대비하는 것이 중요합니다.[1] IT 팀을 축소하면 공격자가 더 손쉽게 성공할 수 있는데, 이는 재무 및 평판에 심각한 영향을 미치게 될 수 있습니다.

이처럼 확장되는 위협 환경에서 성공하기 위한 핵심은 IT 팀에 더 많은 것을 요구하는 것이 아니라, 제로 트러스트 보안 모델의 형태로 강력한 보안 기준을 설정하는 것입니다. 이러한 보안 기반은 IT 팀의 부담을 덜어주고 공격의 위험과 심각도를 줄이는 데 도움이 되지만, 여기에서 이점이 시작됩니다.

이 eBook에서는 일반적인 최신 보안 장벽에 대해 살펴보고 제로 트러스트 보안을 구현하여 조직이 이를 극복하는 데 어떻게 도움이 되는지 설명합니다. 또한 제로 트러스트 보안 모델을 통해 발생하는 긍정적인 파급 효과와 이것이 팀 생산성 및 AI 준비 상태에 미치는 영향에 대해서도 논의해 보겠습니다.

주요 보안 과제

사이버 공격자들은 점점 더 정교해지고 조직화되고 있으며, 악의적인 행위자는 고급 도구와 전술을 사용하여 약점을 찾아 악용하고 있습니다. 사이버 범죄자가 성공할 경우, 특히 침해가 민감한 데이터나 개인 데이터와 관련된 경우 피해자의 평판 및 재정적 피해가 심각할 수 있습니다. 외부적으로는 고객, 파트너, 투자자의 신뢰를 잃게 됨에 따라 시장 점유율이 감소하고 고객 이탈이 발생하며 기업 가치가 낮아질 수 있습니다. 내부적으로는 사이버 공격이 운영을 방해하여 다운타임, 생산성 저하, 수익 손실을 초래합니다.



사이버 범죄로 인한 재정적 피해 증가

$23조 8,400억

전 세계 사이버 범죄의 예상 비용은 2027년까지 **미화 23조 8,400억 달러**에 이를 것으로 예상됩니다.[2]

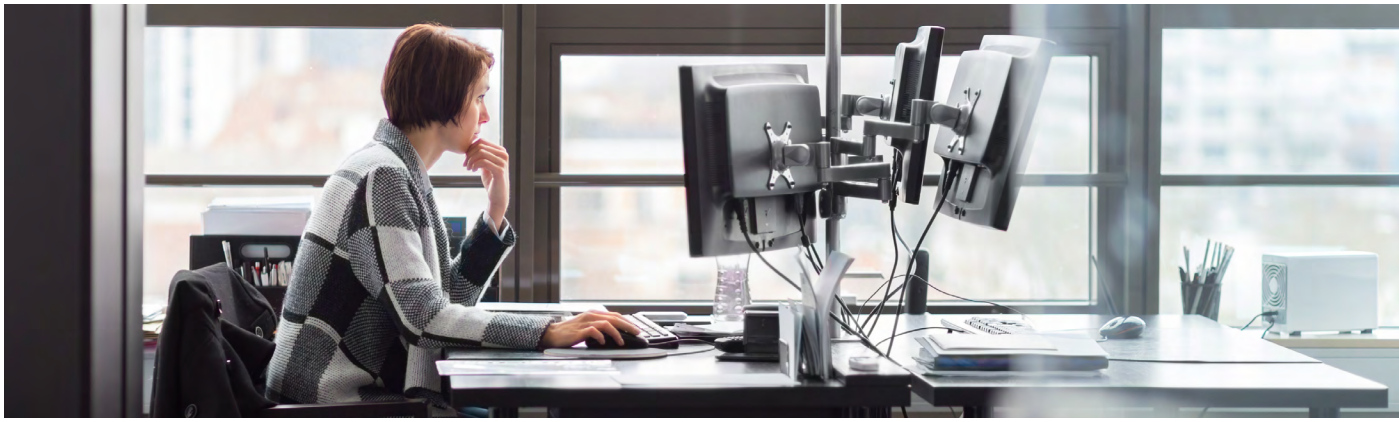
현대 업무에서 나타날 수 있는 주요 보안 문제

이러한 끔찍한 결과에 직면한 IT 팀은 몇 가지 주요 과제에 직면해 있습니다.

ID 확인
공격자는 피싱, 맬웨어, 도메인 스푸핑과 같은 다양한 기술을 사용하여 사용자 개인 인증 정보를 포착합니다. 이러한 개인 인증 정보(암호, 사용자 ID, 이메일 등)는 회사 리소스에 대한 액세스 권한을 확보하거나, 데이터를 훔치거나, 계정을 손상시키는 데 사용됩니다.

1,287건
매초마다 발생한 암호 공격 횟수[3]

3,100만
지난 한 해 동안 월 **3,100만**건으로 증가[4]



현대의 인력 보호
최근 몇 년 동안 많은 기업의 업무 모델이 급격히 변화하여 정규직 직원의 **12.7%**가 현재 재택 근무를 하고 있으며 **28.2%**가 하이브리드 모델을 사용하고 있습니다.[5] 이러한 직원은 위협으로부터 방어하기 위해 항상 적절한 예방 조치를 취하는 것은 아니며, 이로 인해 사이버 범죄자는 더 많은 취약점을 악용할 수 있습니다. 한편, 규정을 준수하지 않는 오래된 하드웨어와 관리되지 않는 디바이스로 작업하면 IT 복잡성이 증가하여 조직이 공격에 더 취약해집니다.

80~90%
관리되지 않는 디바이스를 통해 발생한 랜섬웨어 손상 비율[6]

71%
관리되지 않는 디바이스에서 감염될 가능성이 높은 작업자의 비율[7]

86%
오래된 PC 하드웨어가 조직을 더 취약하게 만든다고 말하는 보안 리더의 비율[8]

정보 보호

사이버 범죄자는 조직의 운영을 방해하거나 영업 비밀, 특허, 상표, 저작권과 같은 지적 재산을 훔쳐 경쟁 우위를 확보하려고 합니다. IP 도용은 금전적 이득, 경제 스파이 또는 산업 파괴 행위로 인해 동기가 부여될 수 있습니다. 소프트웨어 및 펌웨어 패치, 하드웨어 업그레이드, 내외부 보안 취약성 등 조직이 처리해야 하는 '중요한 보안 문제'가 많을수록 가장 소중한 데이터를 대상으로 하는 공격에 대비할 수 있는 시간과 노력이 줄어듭니다.

70%

승인되지 않은 소프트웨어, 앱, 서비스로 인해 손상된 조직의 비율[9]

62%

보안 전략이나 정교한 공격에 대비하는 것과 같은 전략적 업무에 충분한 시간을 할애하지 않는 직원의 비율[10]

조직은 사이버 보안에 대한 사전 예방적이고 탄력적인 접근 방식을 채택하여 복잡하고 진화하는 위협 환경을 탐색해야 합니다. 오늘날 이는 기존의 사후 대응적 프레임워크에서 사전 예방적 제로 트러스트 프레임워크로 전환하는 것을 의미합니다.

1단계
제로 트러스트 보안 기반 구축

제로 트러스트는 **'절대 신뢰하지 말고 항상 확인'**하라는 모토하에 운영되는 보안 모델입니다. 신뢰는 악용 가능한 진입점을 찾는 데 사용할 수 있는 취약점이라는 사실을 인식하고 사이버 범죄자가 의도치 않게 방어를 통과하지 못하도록 가드레일을 설치해야 합니다.

절대 신뢰하지 않음

내부 또는 외부의 엔터티를 절대적으로 신뢰하지 않습니다.

항상 확인함

ID, 디바이스, 데이터, 네트워크에 대한 지속적인 확인이 필요합니다.

제로 트러스트 원칙

회사 방화벽 뒤에 있는 모든 것이 신뢰할 수 있다고 가정하는 대신 제로 트러스트 보안은 조직 리소스에 액세스하려는 모든 엔터티(내부 또는 외부)가 잠재적인 위협이라고 가정합니다. 이러한 가정은 명시적으로 검증하고, 최소 권한 액세스를 구현하며, 위반을 가정하는 세 가지 원칙을 적용해야 합니다.

명시적 검증

첫 번째 원칙은 네트워크에 액세스하려는 사람이 자신이 말하는 사람인지 확인하기 위해 고안되었습니다. 리소스에 대한 모든 액세스 요청은 사용자의 ID, 디바이스, 위치, 액세스하는 서비스 또는 워크로드, 데이터 분류, 식별된 변칙 또는 위험을 비롯한 여러 요인에 따라 인증되고 권한이 부여됩니다. 이렇게 하면 유효한 사용자 및 디바이스가 회사 리소스에 액세스할 수 있으며 의심스러운 엔터티는 차단되거나 질문을 받게 됩니다.

최소 권한 액세스 실현

이 원칙은 사용자가 작업을 완료하는 데 필요한 리소스에 액세스할 수 있도록 지원합니다. 이러한 접근 방식은 권한이 없거나 손상된 사용자 및 디바이스에 대한 중요한 데이터 및 리소스의 노출을 제한하고 공격자가 네트워크 내에서 가할 수 있는 손상 범위를 제한합니다. JIT/JEA(Just-In-Time and Just-Enough Access) 정책, 위험 평가를 기반으로 하는 적응형 정책, 데이터 보호 전략과 같은 방법은 이 원칙을 적용하는 데 도움이 됩니다.

침해 가정

이 원칙은 침해로 인해 발생할 수 있는 피해를 최소화하는 것을 목표로 합니다. 침해를 가정할 때 리소스에 대한 액세스를 세분화하고, 전송 중 및 저장 데이터 암호화를 보장하며, 가시성, 위협 탐지, 방어 강화를 위해 분석을 사용하는 것이 포함됩니다. 이 전략은 공격의 폭발 반경을 줄이고 공격자가 액세스 권한을 확보할 경우 네트워크 내에서 측면으로 이동하는 것을 방지하는 데 매우 중요합니다.

제로 트러스트 원칙 구현을 위한 모범 사례: ID 및 엔드포인트

보호 보안 기반을 구축하려면 Microsoft 365 E3와 같은 최신 생산성 솔루션이 필요합니다. 내장형 제로 트러스트, AI, 자동화 기능이 이에 포함되어 신속하게 ID를 확인하고, 승인된 사용자에게 액세스 권한을 부여하며, 여러 플랫폼에서 위협을 모니터링할 수 있습니다. 제로 트러스트 보안을 구축하려면 ID와 엔드포인트를 보호하는 데 중요한 이 기반을 갖춘 포괄적인 솔루션을 찾아 인력의 생산성을 극대화하고 가장 안전하게 지원하세요.

ID 보호

다중 인증 배포: 사용자가 액세스 권한을 부여받기 전에 두 번째 소스(예: 전화 또는 토큰)를 통해 ID를 확인하도록 요구합니다.

암호 없는 인증 사용: 사용자가 지문 또는 고유 코드와 같은 다른 형태의 증거를 요청하여 암호를 입력하지 않고 ID를 확인하도록 합니다.

SSO(Single Sign-On) 구현: 동일한 사람에 대해 여러 개의 개인 인증 정보를 관리할 필요가 없어 작업자가 다른 애플리케이션을 사용할 때 로그인 프롬프트가 더 적게 표시됩니다.

더 많은 데이터를 통해 ID 및 액세스 관리(IAM) 솔루션 강화: IAM 솔루션에 더 많은 데이터를 제공하여 누가 회사 리소스에 액세스하는지에 대한 가시성을 높일 수 있습니다.

엔드포인트 보호

레거시 인증 차단: 앱 또는 디바이스가 최신 보안 기능을 지원하지 않는 이전 프로토콜을 사용하지 못하도록 차단하여 악의적인 행위자가 도난당하거나 재사용된 개인 인증 정보를 사용하여 리소스에 액세스할 수 없도록 합니다.

실시간 위험 평가 수행: AI, 자동화, 분석을 사용하여 모든 액세스 요청의 위험 수준을 지속적으로 확인 및 평가하여 이상 징후를 실시간으로 탐지하고 완화합니다.

보안 태세를 지속적으로 평가 및 최적화: ID 및 보안 태세를 지속적으로 평가하여 환경이 현재 모범 사례에 얼마나 잘 부합하는지 확인하여 정교한 위협에 미리 대비합니다.

제로 트러스트 보안 모델
구현의 이점

'절대 신뢰하지 않고 항상 확인' 모델을 적용하여 사이버 위협으로부터 더 안전하게 보호하는 방법

더 강력한 보안 태세 구축
제로 트러스트는 공격 표면을 최소화하고 승인되지 않은 액세스를 차단함으로써 일상적인 운영으로 인해 악용 가능한 취약성의 수를 줄입니다. 또한 악의적인 행위자가 액세스 권한을 확보하는 경우 제로 트러스트 보안은 악의적인 행위자의 존재를 감지하고 악의적인 행위자가 가할 수 있는 피해를 사전에 제한하는 데 도움이 됩니다.

최신 업무 생산성 모델을 채택할 수 있는 역량 강화
제로 트러스트는 하이브리드 업무 모델에 적합하며, 직원이 근무하는 장소와 방식에 관계없이 안전한 액세스를 제공합니다. 이렇게 하면 작업자가 새로운 위치에서 작업하거나 디바이스를 전환할 때 리소스에 액세스할 수 없기 때문에 생산성이 중단되는 것을 방지할 수 있습니다.

간소화된 보안 관리
제로 트러스트는 일관된 보안 및 거버넌스 정책에 따라 ID, 앱, 디바이스, 인프라, 데이터를 포괄하는 포괄적인 솔루션을 제공하여 보안 관리를 간소화합니다. 또한 제로 트러스트는 위협 모니터링 및 위험 평가와 같은 작업에 AI 및 자동화를 추가하여 관리를 더욱 간소화하고 IT 팀이 전략적 이니셔티브와 혁신에 집중할 수 있도록 합니다.

Foundry 제로 트러스트 설문 조사 응답자들은 제로 트러스트 모델을 구현하면 생산성, 위험 감소, 규정 준수에 영향을 미치는 이점이 있다고 보고했습니다.[11]

설문 조사 응답자들이 보고한 주요 이점:

- 고객 데이터 보호
- 지속적인 액세스 및 인증
- 클라우드 앱 및 디바이스에 대한 액세스 관리
- 원격 업무로의 전환 촉진
- 보안 기술 부족 문제 해결
- 통합의 복잡성 감소
- 침해 감지 시간 단축
  보안 및 탁월한 최종 사용자 환경 모두 제공

2단계
엔드포인트 관리 간소화

조직에서 제로 트러스트 보안 기반을 구축한 후에는 IT 관리자가 엔드포인트 관리를 간소화할 수 있는 간소화된 프레임워크를 채택할 수 있습니다.

엔드포인트는 데스크톱 컴퓨터, 노트북, 태블릿, 휴대폰, IoT 디바이스, 클라우드 솔루션 등 일상적인 업무에 사용되는 다양한 디바이스를 포함합니다. 엔드포인트의 수는 매년 증가하고 있으며, 현재 평균적으로 기업은 약 **135,000개**의 디바이스를 보유하고 있습니다.[12] 이러한 다양한 엔드포인트를 모두 관리하고 보호하는 것은 IT 헬프 데스크 비용 중 약 30%가 엔드포인트 문제를 해결하는 데 사용되는 크고 비용이 많이 드는 작업입니다. Microsoft 365 E3와 같은 클라우드 기반 생산성 제품군을 사용하면 엔드포인트 디바이스 수가 계속 증가하더라도 엔드포인트 관리를 간소화하고 IT 비용을 절감할 수 있습니다.

간소화된 엔드포인트 관리로 무엇을 달성할 수 있을까요?

직원 환경 및 생산성 강화. 다양한 앱, 주변 장치, 디바이스, 셀프 서비스 옵션에 대한 지원을 제공하여 직원이 어디서나 효율적으로 작업할 수 있도록 합니다.

엔드포인트 성능, 상태, 보안에 대한 제어 개선. ID, 위치, 규정 준수, 위험 요소를 기반으로 하는 최신 운영 체제 및 보안 정책으로 디바이스를 최신 상태로 유지합니다.

IT 복잡성 감소. 클라우드를 활용하여 디바이스 및 애플리케이션 배포, 환경 설정, 업데이트를 간소화하여 IT 효율성을 높입니다. 그 결과, 다양한 운영 체제, 디바이스 유형, 소유권 모델에 걸쳐 엔드포인트에 대한 포괄적인 관리 및 보안이 구현됩니다.

제로 트러스트 기반을 구축하고 엔드포인트 관리를 간소화하는 두 단계를 완료하면 다음 목표인 방해받지 않는 생산성과 협업에 초점을 맞춥니다.

Microsoft 365 E3: 제로 트러스트 보안과 통합형 엔드포인트 관리를 결합하여 인력의 생산성 극대화

과거에 조직은 보안과 생산성 사이에서 신중한 균형을 유지해야 했습니다. IT 부서가 보안 방어 체계를 너무 많이 구축하면 직원들이 필요한 정보와 리소스에 액세스하는 데 어려움을 겪음에 따라 생산성에 영향을 미칠 수 있습니다. 반면, 방어 체계가 너무 적으면 사이버 공격이 한 번만 성공해도 전체 운영이 중단될 수 있습니다.

Microsoft 365 E3는 기본적인 제로 트러스트 보안, 엔터프라이즈급 디바이스 및 앱 관리, 강력한 협업 도구를 제공하는 클라우드 기반 생산성 솔루션입니다. 내장된 AI 기능을 통해 데이터와 지식의 컨텍스트를 이해하여 조직 전체의 안전한 생산성을 강화하여 직원이 모든 수준에서 집중하고, 연결되고, 안전하도록 합니다.

Microsoft 365 E3 기능

중앙에서 ID 및 액세스 관리
사용자가 마찰 지점을 만나지 않고도 필요한 리소스를 확보할 수 있도록 하는 강력한 적응형 액세스 정책을 활성화합니다.

정보 보호 및 거버넌스
저장 중이든, 전송 중이든, 사용 중이든 상관없이 데이터를 암호화된 상태로 유지하고 민감한 정보를 쉽게 검색합니다.

자동화된 위협 방지
업데이트를 자동화하여 소프트웨어를 최신 상태로 유지하고, 패치를 신속하게 배포하여 악용 가능한 취약성을 줄이며, 비즈니스 연속성을 방해하는 위협을 사전에 차단합니다.

생산성 강화:
Microsoft Copilot for Microsoft 365

AI를 사용하려면 다양한 소스에서 수집된 많은 데이터가 필요합니다. 제로 트러스트 보안과 원활한 엔드포인트 관리를 구현하는 것은 모든 데이터를 안전하고 쉽게 관리할 수 있도록 하는 중요한 단계입니다. 이러한 작업이 완료되면 Microsoft Copilot과 같은 도구를 사용하여 생산성을 더욱 높일 수 있습니다.

Microsoft Copilot for Microsoft 365는 문서 작성, 미팅 일정 예약, 프로젝트 관리와 같은 일반적인 작업을 자동화하여 일상적인 작업 시간을 없애는 데 도움이 되는 AI 기반 생산성 도구입니다. 이처럼 시간적인 여유를 통해 직원들은 높은 창의성과 혁신적인 문제 해결이 필요한 작업에 더 많은 시간과 에너지를 쏟을 수 있습니다.

AI를 사용하여 창의성을 위한 공간 마련

70%

워크로드를 줄이기 위해 AI에 최대한 많은 작업을 위임할 의향이 있는 사람의 비율[13]

총 경제적 영향

Forrester Consulting에서 실시한 한 위탁 연구에 따르면 Microsoft 365 E3는 보안을 강화하고 생산성을 높이며 IT 관리를 간소화하는 것으로 나타났습니다.[14]

강력한 보안

35%

데이터 침해 가능성이 줄어들었습니다.

생산성

60HR

Microsoft 365 E3를 통해 연간 평균 60시간을 절약했습니다.

간소화된 IT

25%

새 소프트웨어 배포 및 관리에 소요되는 시간을 25% 까지 단축했습니다.

Microsoft 365의 안전한 생산성을 통해 기업의 역량을 강화하세요.

더 알아보기 ›

[1] IT Trends Report: Remote Work Drives Priorities in 2021. JumpCloud, 2021년.
[2] Chart: Cybercrime Expected To Skyrocket in Coming Years. Statista. 2022년.
[3] Microsoft Security Copilot: How does it help you protect your data? Intelequia. 2023년 4월.
[4] Microsoft Entra: 2023년 ID에 대한 5가지 우선순위. Microsoft Security. 2023년 1월.
[5] Remote Work Statistics & Trends In (2023). Forbes Advisor. 2023년.
[6] Microsoft 디지털 방어 보고서. 2023년.
[7] 최신 공격 표면의 해부학. Microsoft Security Insider. 2023년 5월.
[8] Microsoft Security Signals Boost SDM Research Learnings. Hypothesis Group. 2021년 9월
[9] The State of Attack Surface Management 2022. Randori. 2022년.
[10] Microsoft 디지털 방어 보고서. 2022년.
[11] Zero Trust Adoption Survey. Foundry. 2022년 5월.
[12] Managing Risks and Costs at the Edge. Ponemon Institute. 2022년.
[13] 작업 동향 지수 연간 보고서: AI가 업무 환경의 문제를 해결할 수 있을까요? Microsoft. 2023년 5월.
[14] The Total Economic Impact Of Microsoft 365 E3. Forrester Consulting에서 실시한 연구 조사, 2022년.