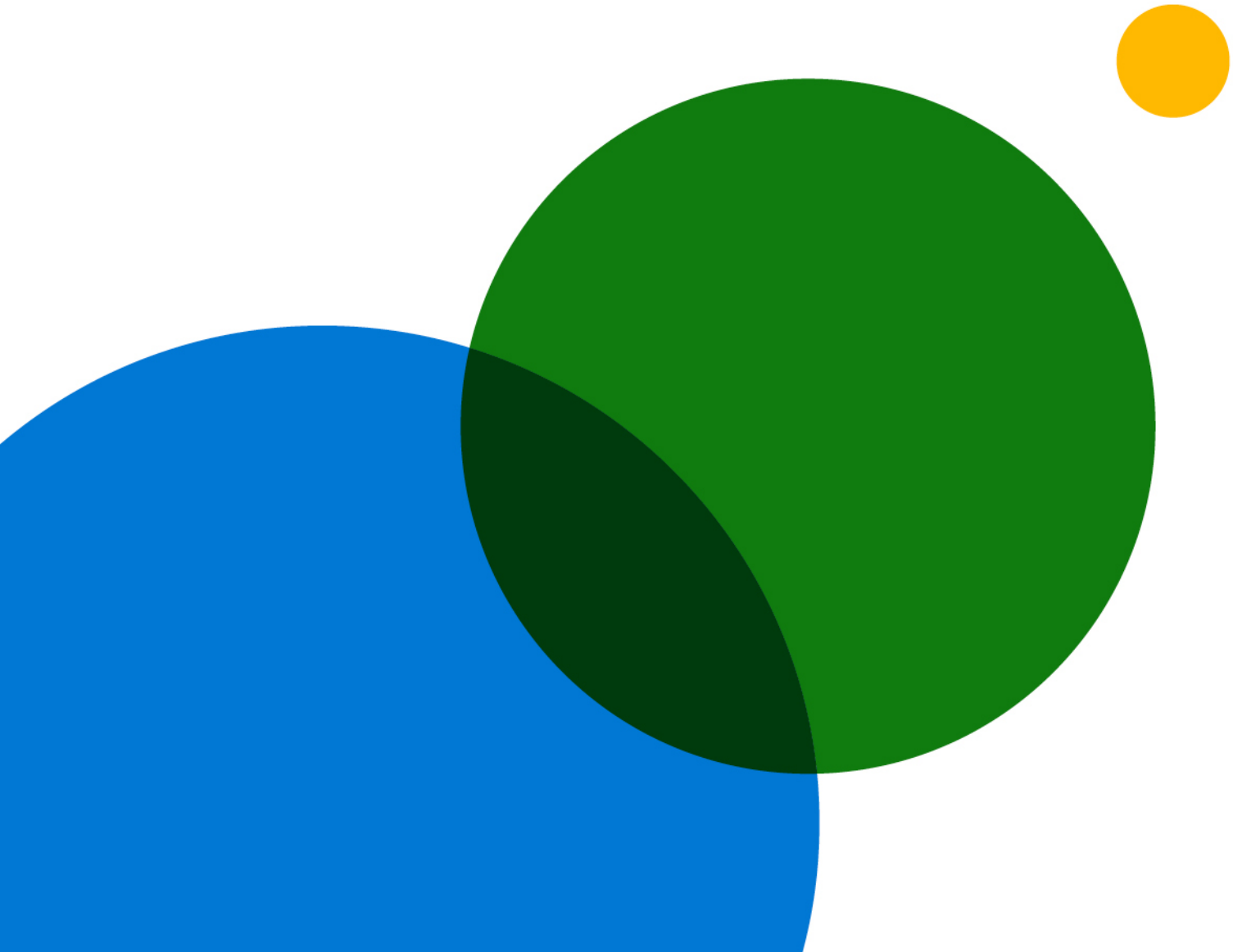
Microsoft Security

hypothesis

# 제로 트러스트 채택 보고서



# 목차

# 소개말

Vasu Jakkal / Microsoft 보안, 규정 준수 및 ID 부문 부사장

지난해 사이버 보안의 발전과 제로 트러스트의 등장은 글로벌 산업과 조직을 위한 지침 전략으로서 놀라운 역할을 수행했습니다.

팬데믹이 시작되었을 때 , 워크플레이스는 하룻밤 사이에 거의 완전히 원격으로 바뀌었습니다. 이러한 변화로 인해 많은 조직은 개인 디바이스를 이용하고, 클라우드 서비스를 통해 협업하며, 기업 네트워크 경계 밖에서 데이터를 공유하여 작업을 수행하는 직원들을 지원하기 위해 신속하게 적응해야 했습니다. 조직은 이러한 변화에 적응하는 동시에 목표, 전술 및 리소스를 지속적으로 발전시키면서 점점 더 정교해지는 사이버 범죄자에 맞서야 했습니다.

오늘날 하이브리드 업무는 새로운 현실입니다. 조사에 참여한 조직들은 이러한 배경과 급격한 변화에 대응하여 보안 및 규정 준수 민첩성 향상, 위협 감지 및 수정 속도 증가, 보안 분석의 단순성 및 가용성 향상을 위해 제로 트러스트에 의존한다고 말했습니다.

포괄적인 제로 트러스트 아키텍처는 명시적으로 검증하고, 최소 권한 액세스를 이용하며, 침해를 가정하는 원칙을 기반으로 ID, 엔드포인트, 앱, 인프라, 네트워크 및 데이터 내부 및 전반에서 향상된 가시성, 자동화 및 오케스트레이션으로 협력하여 보호 장치를 구축합니다. Microsoft는 이러한 접근 방식을 고객 및 파트너에게 권장할 뿐만 아니라 글로벌 보안 및 소프트웨어 개발에 대한 Microsoft 접근 방식으로 수용했습니다.

이 보고서는 다양한 시장과 산업에서 제로 트러스트 채택의 경로를 조명합니다. 이 연구를 통해 얻은 교훈이 제로 트러스트 전략 채택을 가속화하고, 동료의 집단적 발전을 조명하며, 빠르게 발전하는 세상의 미래 상태에 대한 인사이트를 제공하는 데 도움이 되기를 바랍니다.

# 방법론

Microsoft는 인사이트, 디자인 및 전략 분석 기관인 Hypothesis Group에 의뢰하여 제로 트러스트 채택 보고서를 작성하고 관련 연구를 수행했습니다. 이 연구는 제로 트러스트 채택의 동향과 모멘텀을 강조하기 위해 미국의 두 단계를 포함했으며, 글로벌 동향을 파악하기 위해 두 번째 단계에서 미국 외 시장이 추가되었습니다.

초기 연구는 2020년 8월 다양한 산업 분야의 엔터프라이즈급 기업에서 제로 트러스트 전략 결정에 참여하는 300명의 SDM(보안 의사 결정자)을 대상으로 미국에서 15분 간의 온라인 설문 조사로 진행되었습니다. 온라인 설문 조사 외에도 2020년 9월 다양한 산업 분야의 미국 SDM을 대상으로 5건의 심층 온라인 인터뷰를 진행했습니다.

2021년 4월에는 미국, 독일, 일본, 호주/뉴질랜드에서 유사한 보안 의사 결정자 그룹을 대상으로 글로벌 연구를 수행했습니다. 900명 이상의 참가자가 15분 간의 온라인 설문 조사에서 제로 트러스트 전략 채택, 모범 사례, 이점, 과제 및 미래 투자 의사에 대한 질문에 응답했습니다.

# 제로 트러스트 채택에 대해 알아야 할 사항

### 01 / 조직은 하이브리드 워크스페이스로의 전환과 코로나19로 가속화된 제로 트러스트 전략을 활용할 준비가 되어 있습니다.

SDM(보안 의사 결정자)은 제로 트러스트 전략을 개발하는 것이 최우선 보안 과제라고 말하며, 96%가 조직의 성공에 매우 중요하다고 답했습니다. 제로 트러스트 전략을 채택하는 주요 동기요인은 전반적인 보안 태세와 최종 사용자 환경을 개선하는 것입니다. 코로나19로 인해 가속화된 하이브리드 워크플레이스로의 전환은 제로 트러스트 전략의 광범위한 채택을 주도하고 있습니다. 기업 조직의 81%가 하이브리드 워크플레이스로 전환하기 시작했으며, 31%는 하이브리드 워크플레이스로 완전히 전환했습니다. 그러나 94%는 주로 전환, 직원의 남용, IT 워크로드 증가 및 사이버 공격에 대해 우려하고 있습니다. 이를 감안하면 전략에 대한 주요 고려 사항에는 원활한 사용자 환경과 전환을 보장하기 위한 직원 및 다중 인증에 대한 교육 증가가 포함됩니다.

### 02 / 조직은 제로 트러스트 전략으로 구현을 시작할 수 있는 유연성을 통해 접근 방식을 필요에 맞게 조정할 수 있습니다.

15% 미만의 조직만이 동일한 보안 위험 영역에서 제로 트러스트 전략을 구현하기 시작했습니다. 이는 전략 구현이 일련의 서로 다른 개별 기술이 아닌 보안 아키텍처의 여러 부분과 기능 전반에서 엔드 투 엔드 프로세스로서 접근하기 때문입니다. 마찬가지로 보안 위험 영역 내에서 제로 트러스트의 개별 구성 요소가 구현되는 순서는 매우 가변적이며, 먼저 구현되는 구성 요소는 보안 전문가마다 매우 다릅니다.

### 03 / 제로 트러스트 전략이 널리 채택되고 조직의 위협 관리 능력을 개선했지만 여전히 해야 할 일이 남아 있습니다.

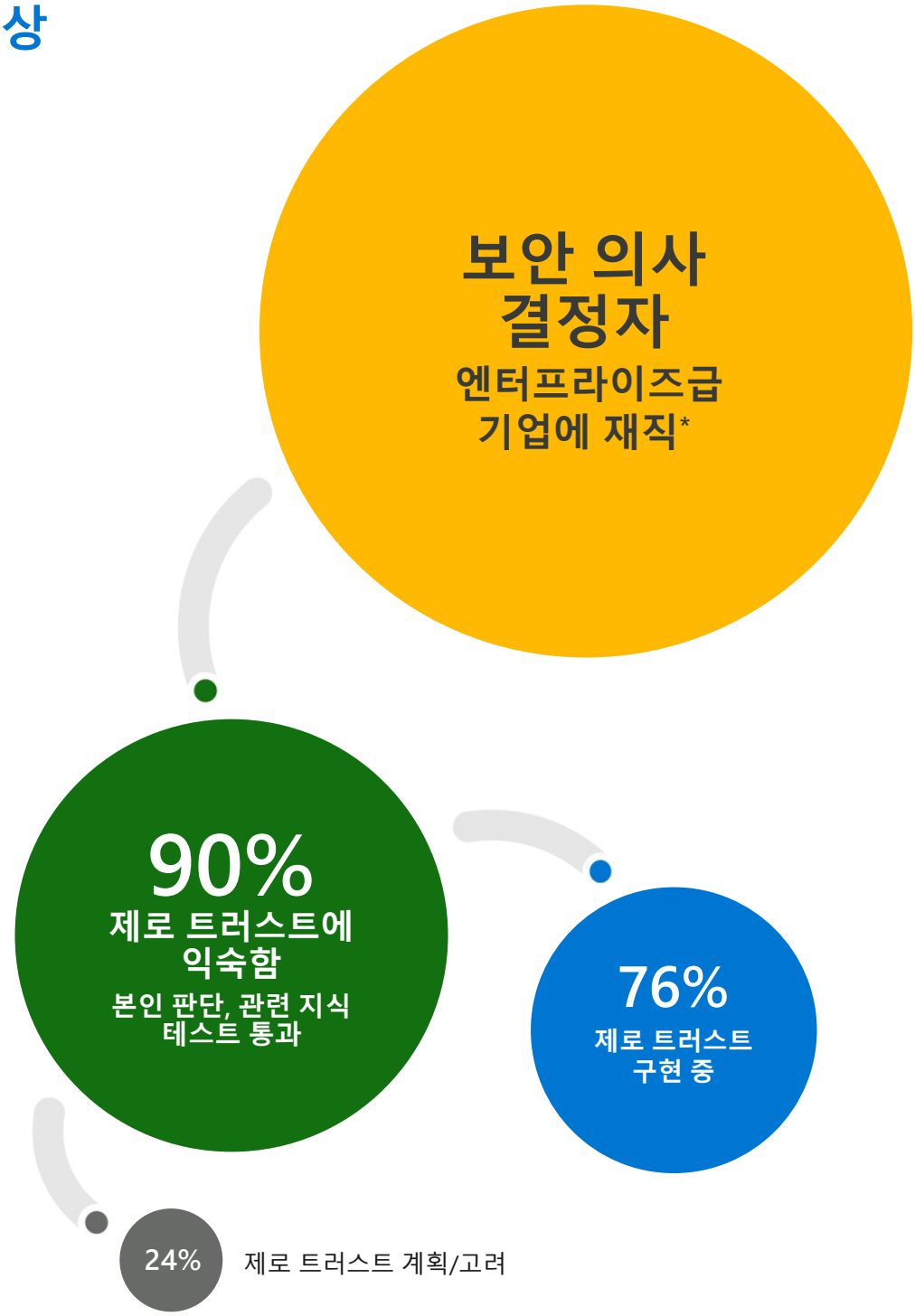
조직의 76%가 최소한 제로 트러스트 전략을 구현하기 시작했고, 35%는 완전히 구현했다고 주장합니다. 그러나 완전히 구현했다고 주장하는 조직들도 모든 보안 위험 영역 및 구성 요소 전반에서 제로 트러스트 전략을 구현하지는 못했다고 인정합니다. 제로 트러스트 전략은 민첩성 향상, 위협 감지 속도, IoT 및 OT(운영 기술) 보안을 관리하는 개선된 기능을 제공하기 때문에 강력합니다. 미국에서 제로 트러스트 채택률은 2020년 8월 70%에서 2021년 4월 79%를 기록하며 증가하고 있습니다. 또한 미국은 채택을 늦게 시작한 다른 국가들에 비해 제로 트러스트 구현에 더 앞서 있으며, 미국의 조직들은 예산에 덜 제한적이라고 주장합니다. 57%의 조직이 채택과 관련하여 다른 조직보다 앞서 있다고 주장하지만, 이 중 절반 정도는 모든 보안 위험 영역 및 구성 요소에서 제로 트러스트를 완전히 구현하지 못했기 때문에 여전히 해야 할 일이 남아 있습니다.

### 04 / 제로 트러스트 전략은 앞으로도 최우선 과제로 남아 있을 것이며, 직원과 공급업체에 대한 신중한 의사 결정이 필요합니다.

제로 트러스트 전략은 앞으로 2년 동안 최우선 보안 과제로 남아 있을 것으로 예상되며, 조직은 제로 트러스트에 대한 투자를 증가시킬 것으로 예상합니다. 직원들(직원 보안 팀 및 리더십의 지원 포함)과 함께 과제를 극복하는 것이 제로 트러스트 투자의 효과가 배가되는 열쇠일 것입니다. 공급업체 전략과 관련하여 보안 의사 결정자는 공급업체 선정이 종종 내부 전문 지식의 가용성에 달려 있다는 점을 감안하여 전체적이거나 통합된 공급자와 협력하는 것을 다소 선호합니다. 제품군을 최대로 활용하는 접근 방식의 이점으로는 향상된 전문 지식, 리소스 및 단순성 등이 있지만 구현하는 데 시간이 오래 걸리고, 기존 보안 아키텍처와 통합하기가 더 어려우며, 잠재적인 취약점이 증가될 수 있습니다.

# 인터뷰 대상

글로벌




*1000명 이상,
독일, 일본, 호주/뉴질랜드는

# 전반적인 연구 결과

# 조직은 제로 트러스트 전략을 활용할 준비가 되어 있습니다.

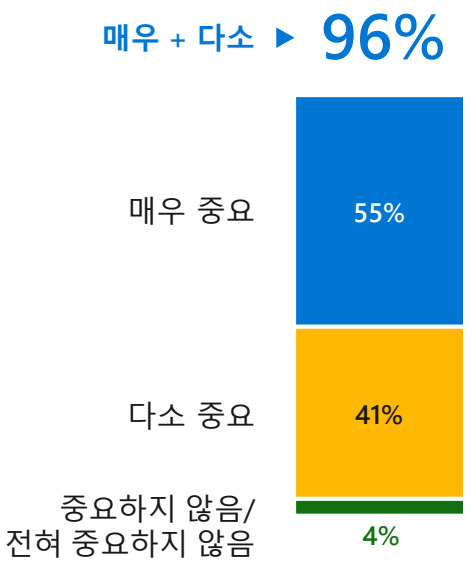
최근 몇 년 동안 수많은 기업에서 채택하고 있는 제로 트러스트 전략은 오늘날 시장과 산업 전반에서 최우선 보안 과제입니다. 53%의 조직이 제로 트러스트를 모든 것 중 최우선 과제라고 생각하지만, 미국(56%)과 독일(53%)의 조직들이 특히 높은 우선 순위를 두고 있습니다.

거의 모든 보안 전문가(96%)는 제로 트러스트 전략이 조직의 성공에 핵심이라고 생각합니다. (붙임 1 참조) 보안 전문가들은 전반적인 보안 태세를 강화하고 최종 사용자 환경을 개선하는 것 외에도 직원들의 보안 절차를 간소화하기 위해 제로 트러스트 전략을 모색하고 있습니다. (붙임 2 참조)

접객업에 종사하는 미국의 한 보안 의사 결정자는 다음과 같이 설명합니다. "*전반적인 보안 태세를 개선하는 것이 목표이지만, 최종 사용자 환경의 마찰을 줄이고 최종 사용자의 삶을 더 편하게 만드는 것이 목표입니다.*"

또한, 보안 전문가의 31%가 코로나19 이후 하이브리드 워크플레이스로의 전환이 임박한 상황에서 제로 트러스트 전략을 중요한 도구로 생각하고 있습니다. 이러한 경향은 호주/뉴질랜드(44 %)에서 특히 두드러집니다.

**붙임 1. 제로 트러스트의 중요성**




**붙임 2. 제로 트러스트 동기요인**

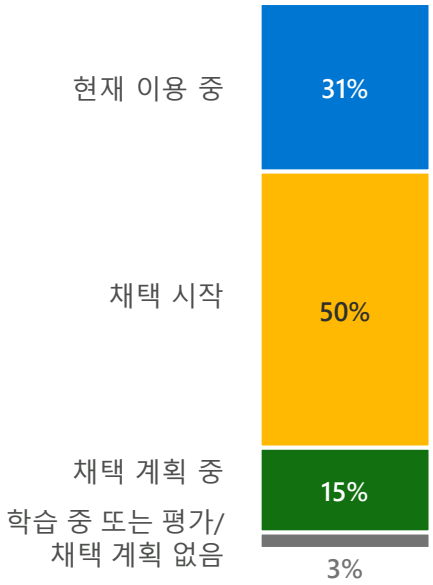
| 상위 동기요인 | |
|---|---|
| 전반적인 보안 태세 개선 | 47% |
| 최종 사용자 환경 및 생산성 향상 | 44% |
| 보안 팀이 협력하는 방식 혁신 | 38% |
| 보안 스택 간소화 | 35% |
| 보안 비용 절감 | 35% |

# 하이브리드 워크플레이스로의 전환으로 인해 제로 트러스트 전략이 광범위하게 채택되고 있습니다.

기업 조직의 81%가 하이브리드 워크플레이스로 전환하기 시작했으며, 31%는 전환을 완료했습니다. 즉, 시장 전반에서 채택 완료율은 일관적이지 않습니다. 호주와 뉴질랜드가 37%로 채택 완료율이 가장 높은 반면 독일은 20%의 조직만이 하이브리드 모델로 전환하여 많이 뒤처져 있습니다. (붙임 3 참조)

글로벌 시장에서 하이브리드 워크스페이스로 전환하는 비율이 서로 다르지만, 전환을 완료하지 않은 조직의 대다수(91%)는 향후 5년 안에 완료할 것으로 예상하고 있습니다. 결정적으로, 94%의 조직에서 직원 남용, IT 워크로드 증가, 사이버 공격의 위험 증가 등으로 인해 전환에 대해 우려하고 있습니다. (붙임 4 참조)

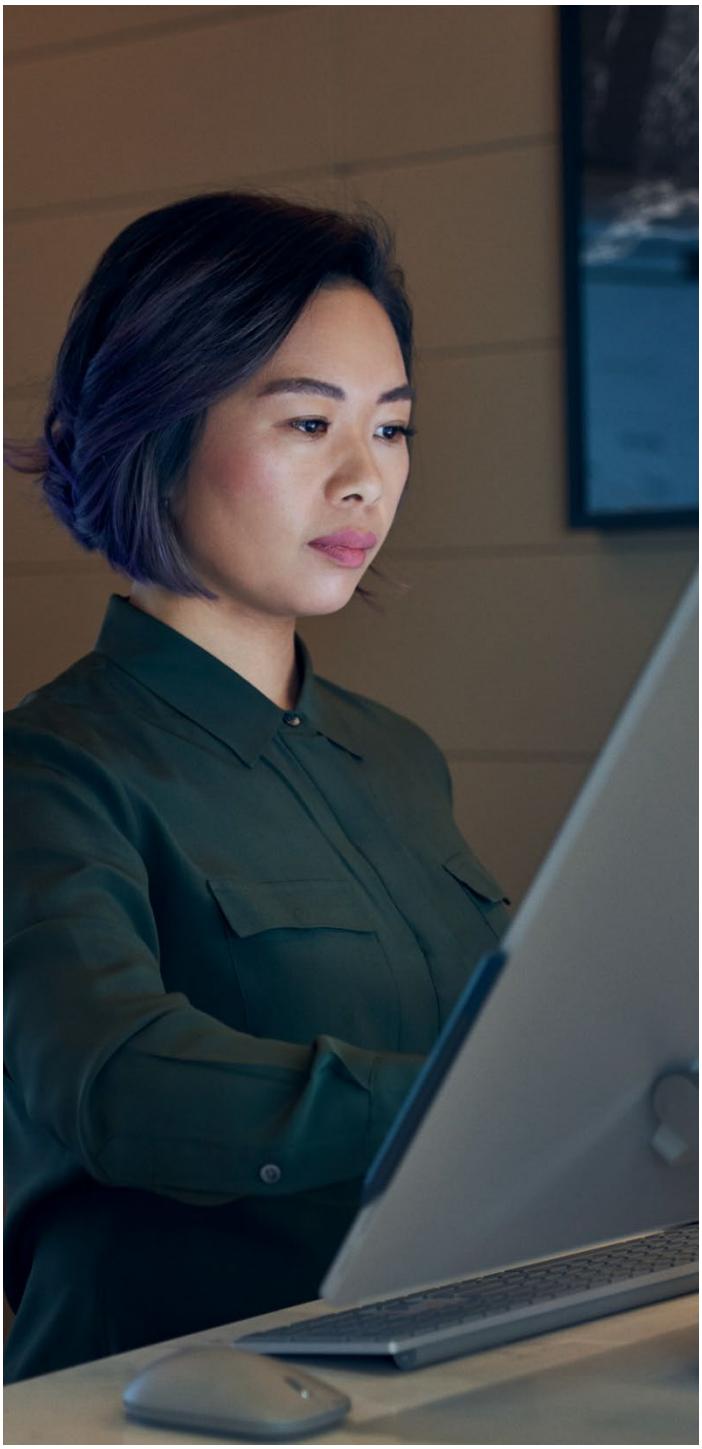
**붙임 3. 하이브리드 워크플레이스 채택 현황**




**붙임 4. 하이브리드 워크플레이스에 대한 우려**

| | |
|---|---|
| 안전하지 않은 앱을 다운로드하는 직원 | 37% |
| IT 워크로드 증가 | 37% |
| 랜섬웨어 공격 | 36% |
| 피싱 공격 | 35% |
| 개인 디바이스의 부적절한 이용 | 34% |
| 데이터에 대한 무단 액세스 | 31% |
| 불가능한 모든 디바이스 관리 | 30% |
| 개인 이메일 계정 이용 | 30% |
| 데이터 규정 준수 불이행 | 24% |

# 코로나19로 제로 트러스트 전략으로의 이동을 가속화하는 새로운 고려 사항이 발생했습니다.



잠재적인 문제를 최소화하기 위한 노력의 일환으로 이해관계자들은 원활한 사용자 환경과 전환을 보장하기 위해 직원(54%)(일본(61%), 독일(58%)) 및 다중 인증(50%)(미국(52%), 독일(56%))에 대한 교육을 증가시키는 것이 중요하다고 강조합니다.

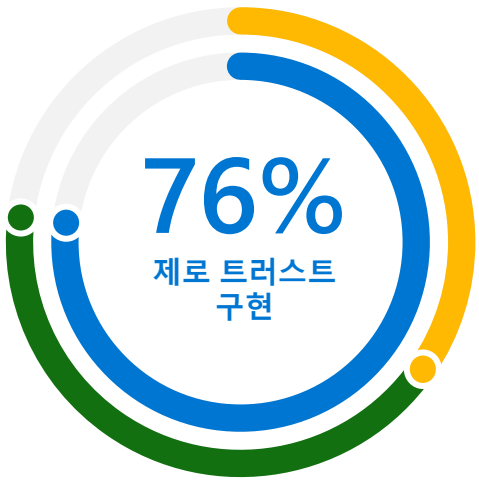
제로 트러스트 전략으로 안전한 원격 및 하이브리드 업무를 지원할 수 있기 때문에 코로나19로 인해 발생한 시장 간 비대칭에도 불구하고 72%의 조직에서 제로 트러스트 전략 채택을 가속화했습니다. 코로나19로 인해 미국(76%), 일본(71%), 호주/뉴질랜드(69%) 등 약 70%의 조직에서 제로 트러스트 전략을 채택했지만, 독일(62%)에서는 하이브리드 워크플레이스로의 전환이 늦어지면서 유독 낮은 구현률을 기록했습니다.

# 제로 트러스트는 전 세계적으로 널리 구현되었고 미국에서도 구현이 늘고 있습니다.

제로 트러스트는 단순한 유행어가 아닌 현실입니다. 조직의 76%에서 제로 트러스트 전략을 구현하기 시작했으며, 35%는 완전히 구현했다고 생각합니다. 그러나 이 데이터는 구현을 완료했다고 간주하는 많은 조직들이 모든 보안 위험 영역에서 구현을 완료하지 않았기 때문에 지나치게 낙관적인 수치입니다. 오늘날 미국은 다른 시장에 비해 제로 트러스트 전략 채택에 앞서 있으며 지속적으로 빠르게 성장하고 있습니다. 미국의 제로 트러스트 전략 구현율은 2020년 8월 70%에서 불과 8개월 만에 79%로 증가하면서 큰 폭으로 성장했습니다. (붙임 5 참조)

현재 제로 트러스트 전략이 보안 분야를 지배하고 있지만, 제로 트러스트의 보편성은 비교적 새로운 것입니다. 기업의 82%가 지난 3년 동안 제로 트러스트 전략을 구현했으며, 21%가 지난 1년 안에 제로 트러스트 전략을 구현했습니다. 미국 조직의 26%가 3년 전부터 구현을 시작한 반면 일본 조직의 19%, 호주/뉴질랜드 조직의 6%, 독일 조직의 3%가 구현을 시작했습니다. 예산 제약이 적은 미국의 초기 구현율은 다른 시장과 비교하여 미국의 조직들이 제로 트러스트 채택에 앞서 있는 이유를 설명할 수 있습니다. 비슷한 맥락에서, 비교적 초기 단계에 있는 독일의 제로 트러스트는 낮은 채택률을 맥락화할 수 있습니다. 독일 조직의 97%가 지난 3년 동안 구현을 시작하기만 했을 뿐입니다.

**붙임 5. 제로 트러스트 구현**



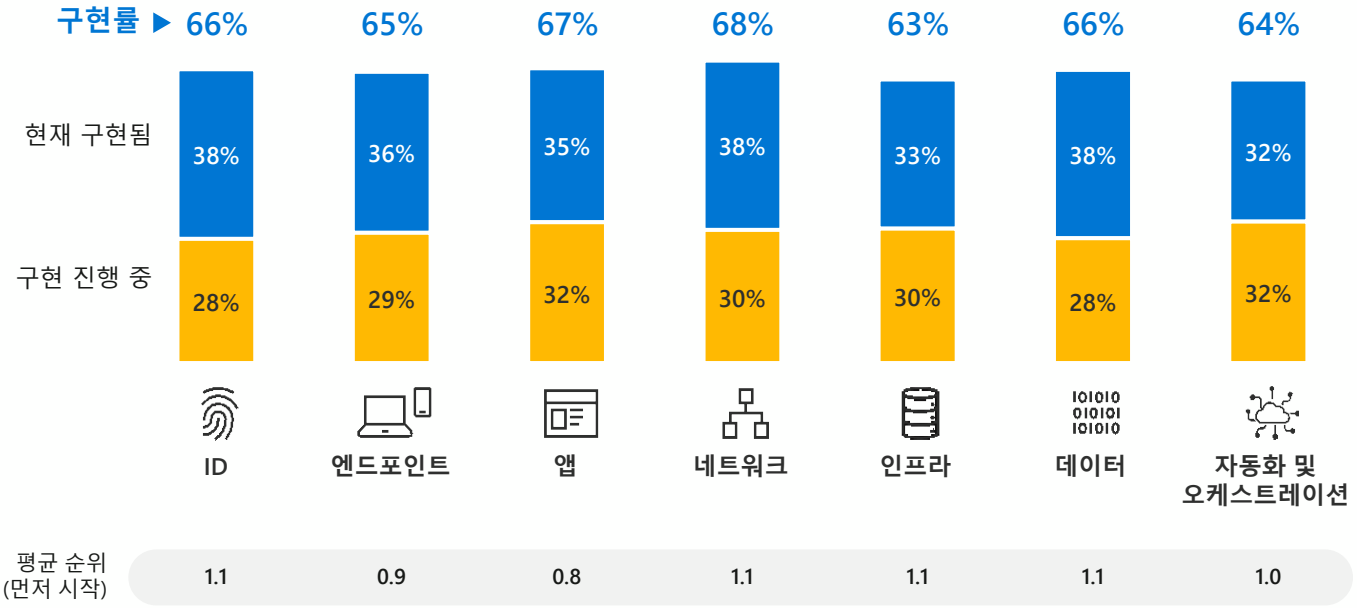

| | 미국 (2020년) | 미국 | 독일 | 일본 | 호주/ 뉴질랜드 |
|---|---|---|---|---|---|
| 제로 트러스트 구현 | 70% | 79% | 75% | 76% | 71% |
| • 구현 완료 | 27% | 44% | 19% | 32% | 28% |
| • 구현 진행 중 | 43% | 35% | 56% | 44% | 43% |

# 제로 트러스트 구현에 대해 모든 상황에 적합한 단일 접근 방식은 없으므로 어디서나 시작할 수 있습니다.

단일 보안 위험 영역(ID, 엔드포인트, 앱, 네트워크, 인프라, 데이터, 자동화 및 오케스트레이션)은 15% 미만이 동일한 보안 위험 영역으로 시작하므로 제로 트러스트 전략의 기본 출발점으로 부각되지 않습니다. 조직은 필요와 이용 가능한 내부 리소스를 기반으로 서로 다른 장소에서 시작하고 있습니다. 결국, 조직은 위협을 더욱 방지하기 위해 모든 보안 위험 영역에서 제로 트러스트 전략을 채택하고자 하므로 제로 트러스트는 시간이 지남에 따라 완료해야 하는 엔드 투 엔드 전략으로 인식되고 있습니다. (붙임 6 참조)

조직은 제로 트러스트 전략의 보안 위험 영역을 넘어 우선 순위를 지정하기 위해 각 보안 위험 영역의 개별 구성 요소를 파악해야 합니다. 엔드포인트, 앱, 네트워크, 데이터 및 자동화/오케스트레이션에는 명확한 출발점이 없습니다. 보안 전문가는 최우선 과제로 평가되는 구성 요소의 위치에 따라 크게 달라집니다. 그러나 일반적으로 ID에 대한 강력한 인증이 먼저 구현되며, 위협 감지 도구는 인프라에서 명확한 우선 순위입니다. (붙임 7 참조)

**붙임 6. 현재 제로 트러스트 구현 상태 – 보안 위험 영역**



## 붙임 7. 제로 트러스트 구성 요소 구현(상위 3개) – 최우선 순위(가장 먼저 구현)

| ID | |
|---|---|
| 강력한 인증(예: 다중 인증, 암호 없는 인증) | 32% |
| 자동화된 위험 감지 및 수정 | 27% |
| 리소스에 대한 게이트 액세스 관련 적응형 액세스 정책 | 22% |

| 엔드포인트 | |
|---|---|
| 관리되거나 관리되지 않는 모든 디바이스에 대한 데이터 손실 방지 정책/제어 | 27% |
| 실시간 디바이스 위험 평가 / 엔드포인트 위협 감지 | 26% |
| ID 공급자에 등록된 디바이스 | 24% |

| 앱 | |
|---|---|
| 진행 중인 Shadow IT Discovery 및 위험 평가 | 23% |
| 앱에 대한 세분화된 액세스 제어 (예: 제한된 가시성 또는 읽기 전용) | 22% |
| 앱에 대한 정책 기반 액세스 제어 | 20% |

| 네트워크 | |
|---|---|
| 네트워크 보호를 위한 보안 액세스 제어 | 25% |
| 컨텍스트 기반 신호를 통한 위협 방지 및 필터링 | 24% |
| 모든 트래픽 암호화 | 20% |

| 인프라 | |
|---|---|
| 보안 운영 팀의 위협 감지 도구 액세스 | 25% |
| 하이브리드 및 다중 클라우드 전반에서 클라우드 워크로드 보호 | 19% |
| 모든 워크로드(가상 컴퓨터, 서버 등)에서 세분화된 가시성 및 액세스 제어 | 17% |

| 데이터 | |
|---|---|
| 보안 정책 엔진으로 제어되는 액세스 결정 | 21% |
| 데이터 분류 및 레이블 지정 | 21% |
| 가장 중요한 파일을 암호화를 통해 지속적으로 보호 | 20% |

| 자동화 및 오케스트레이션 | |
|---|---|
| 조사 및 대응을 위한 중앙 집중식 플랫폼으로 엔드 투 엔드 가시성 구축 | 29% |
| 위협 데이터를 여러 도메인(ID, 엔드포인트, 앱, 네트워크, 인프라)에서 수집 및 분석 | 28% |
| 자동화된 조사와 대응 지원 | 22% |

"저희는 제로 트러스트를 단지 일련의 기술이 아닌, 네트워크 내부 또는 외부의 모든 사용자 리소스를 검증할 수 있을 때까지 신뢰할 수 없는 것으로 처리하기 위한 전략과 접근 방식으로 간주했습니다."

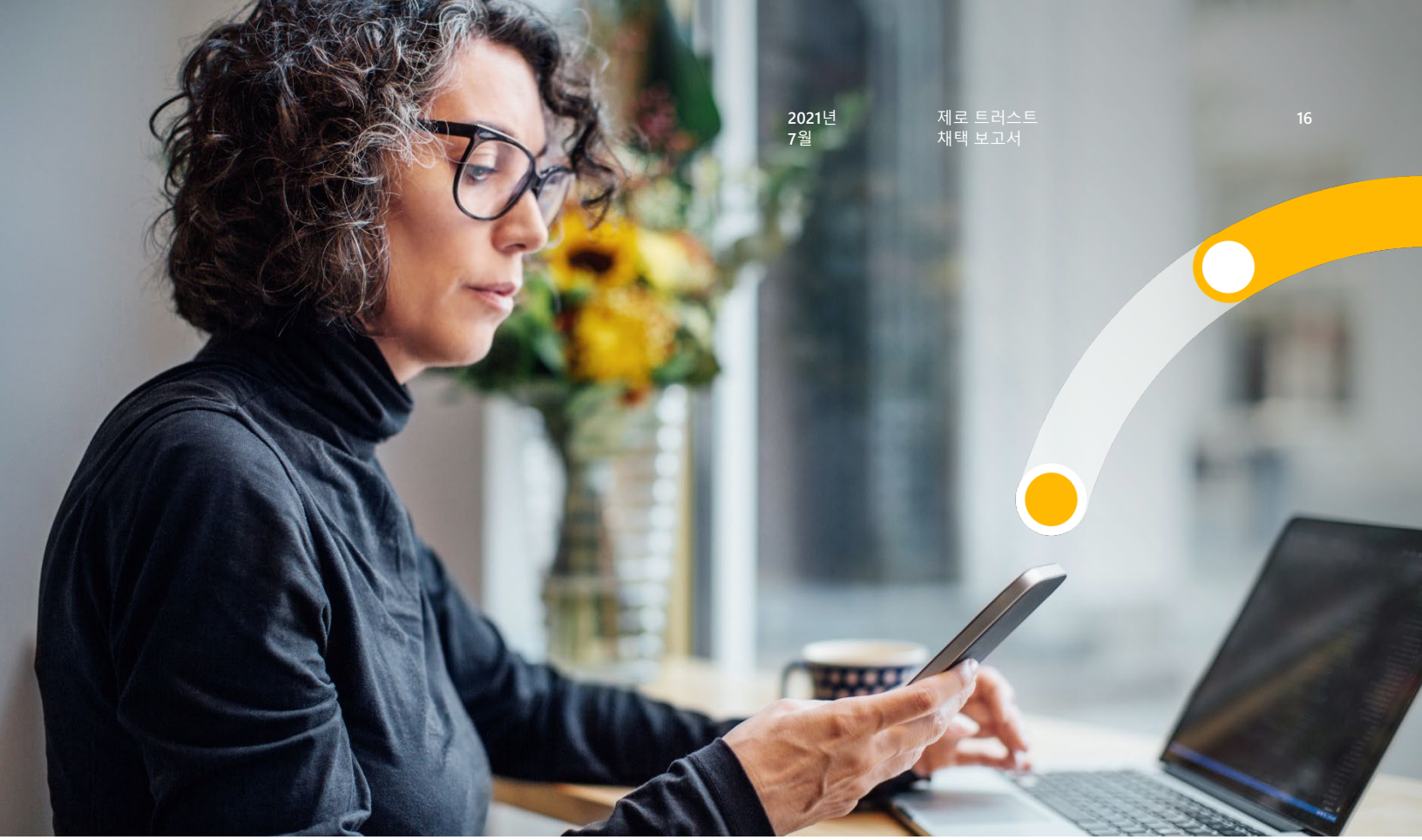
미국의 보안 의사 결정자
접객업

## 조직이 제로 트러스트 전략을 구현하기 시작하면 민첩성, 속도 및 보호가 향상되는 이점이 있지만, 리소스에 대한 이점은 비교적 일반적이지 않습니다.

제로 트러스트 전략이 구현되면 조직은 민첩성 증가(37%), 속도(35%), 고객 데이터 보호(35%)의 이점을 누릴 수 있습니다. (붙임 8 참조) 그러나 해방된 보안 팀(27%)과 인프라 관리를 위한 리소스 요구 감소(22%)를 비롯하여 직원에게 이점이 직접적으로 실현되지는 않습니다.

조직에서 제로 트러스트 전략이 특히 IoT 및 OT 보안(47%)과 관련하여 대부분의 위협과 환경에 대한 변화를 관리하는 데 도움이 된다고 믿는 것이 중요합니다.

**붙임 8. 제로 트러스트의 이점**



## 조직은 제로 트러스트 전략을 최대한 활용하는 데 자신감을 느낍니다.

79%의 조직이 전체적으로 보안 위협을 처리하는 능력에 자신 있지만, 이러한 자신감은 위협이 진실의 조작을 포함한 경우 약해집니다. SDM은 위조 ID(20%)과 딥페이크(10%)와 같은 위협에 대처하는 것에 대해 가장 자신 없다고 생각합니다.

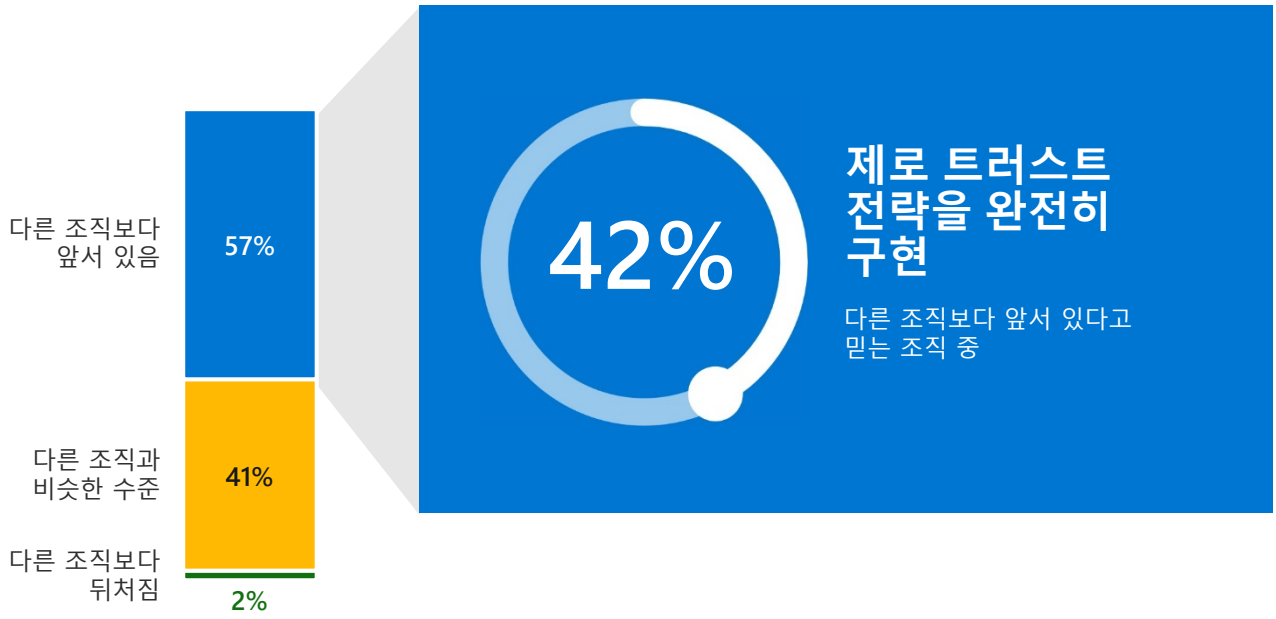
얻은 이점을 고려할 때 제로 트러스트는 일반적으로 긍정적인 연관성을 확보합니다. 4개 시장에서 SDM은 조직의 접근 방식이 실용적인 동시에 열망적이라고 생각하며, 이를 '자신감'(37%)과 '효율적'(31%) 뿐만 아니라 '동기 부여'(25%), '영감'(25%), '흥미 있는'(25%) 등으로 설명합니다. 특히 일본의 보안 전문가들은 제로 트러스트를 '까다로운'(27%)과 '혁신적인'(25%)으로 묘사합니다. 이는 구현하기 쉽지는 않지만 채택된 후의 이점이 광범위하다는 것을 시사합니다.

# 많은 조직들이 제로 트러스트 구현에 앞서 있다고 생각하지만 여전히 해야 할 일이 많습니다.

조직의 35%만이 제로 트러스트 전략을 완전히 구현했다고 답했고, 52%는 계획한 것보다 앞서 있다고 답했으며, 57%는 다른 조직보다 구현에 앞서 있다고 생각합니다. 특히 일본(66%)과 호주/뉴질랜드(63%)의 조직들은 다른 조직보다 앞서 있다고 생각합니다. 시장 전반에서 자신감이 넘쳐나지만, 다른 조직보다 앞서 있다고 느끼는 조직 중 42%만이 제로 트러스트 전략을 완전히 구현했다고 주장하는 것을 감안하면 인식과 현실 사이에 격차를 확인할 수 있습니다. (붙임 9 참조)

많은 조직이 제로 트러스트 전략에 대해 자신 있으며 향후 보안 위협을 처리할 준비가 되어 있지만, 위험 영역 전반에서 완전히 구현하기 위해 해야 할 작업이 여전히 남아 있습니다. 예를 들어, 제로 트러스트 전략을 완전히 구현했다고 간주하는 조직 중 거의 절반이 현재 보안 위험 영역 전체에서 구현하지 못했으며, 특히 인프라와 ID가 구현될 가능성이 가장 낮습니다.

**붙임 9. 제로 트러스트 구현 비교**



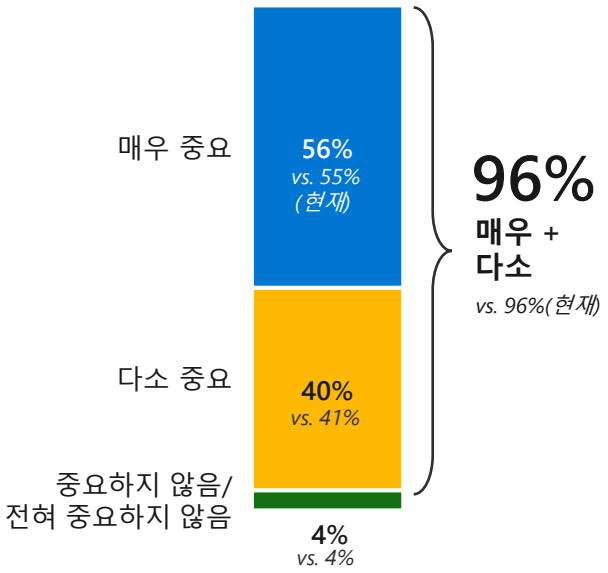

| | 미국 | 독일 | 일본 | 호주/뉴질랜드 |
|---|---|---|---|---|
| 앞서 있음 | 59% | 46% | 66% | 63% |
| 비슷함 | 40% | 52% | 34% | 32% |
| 뒤처짐 | 2% | 2% | 0% | 6% |

# 향후 2년 동안 제로 트러스트 전략은 최우선 보안 과제일 것입니다.

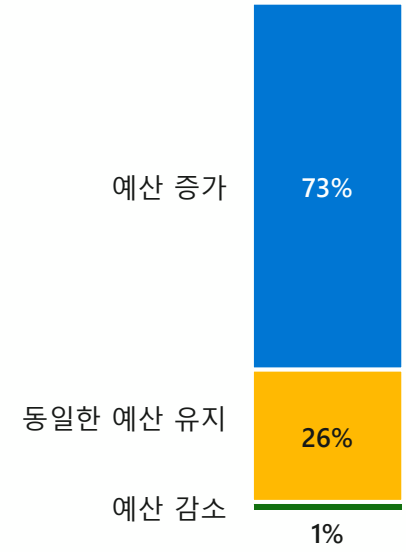
조직은 제로 트러스트 전략에 올인하고 있으며, 의사 결정자들은 향후 2년 동안 최우선 과제일 것이라고 말합니다. SDM들은 제로 트러스트 전략이 전체적인 성공(96%)에 지속적으로 중요한 요소일 것이라고 예상하기 때문에, 보안 이니셔티브로서 제로 트러스트 전략의 상대적인 중요성은 2023년까지 53%에서 58%로 증가할 것으로 예상됩니다. (붙임 10 참조)

예상 중요성은 특히 일본 조직에서 향후 2년 동안 제로 트러스트 전략이 매우 중요하다는 응답이 70%를 기록하며 전체 평균 56%에 비해 높은 수치를 나타냈습니다. 제로 트러스트 전략 예산도 증가할 것으로 예상되며, 73%의 조직이 예산을 늘릴 것으로 예상하고 있습니다. 이 수치는 독일(67%)에서 다소 낮지만, 31%는 예산이 동일하게 유지될 것으로 예상합니다. (붙임 11 참조)

**붙임 10. 향후 2년 동안 제로 트러스트의 예상 중요성**

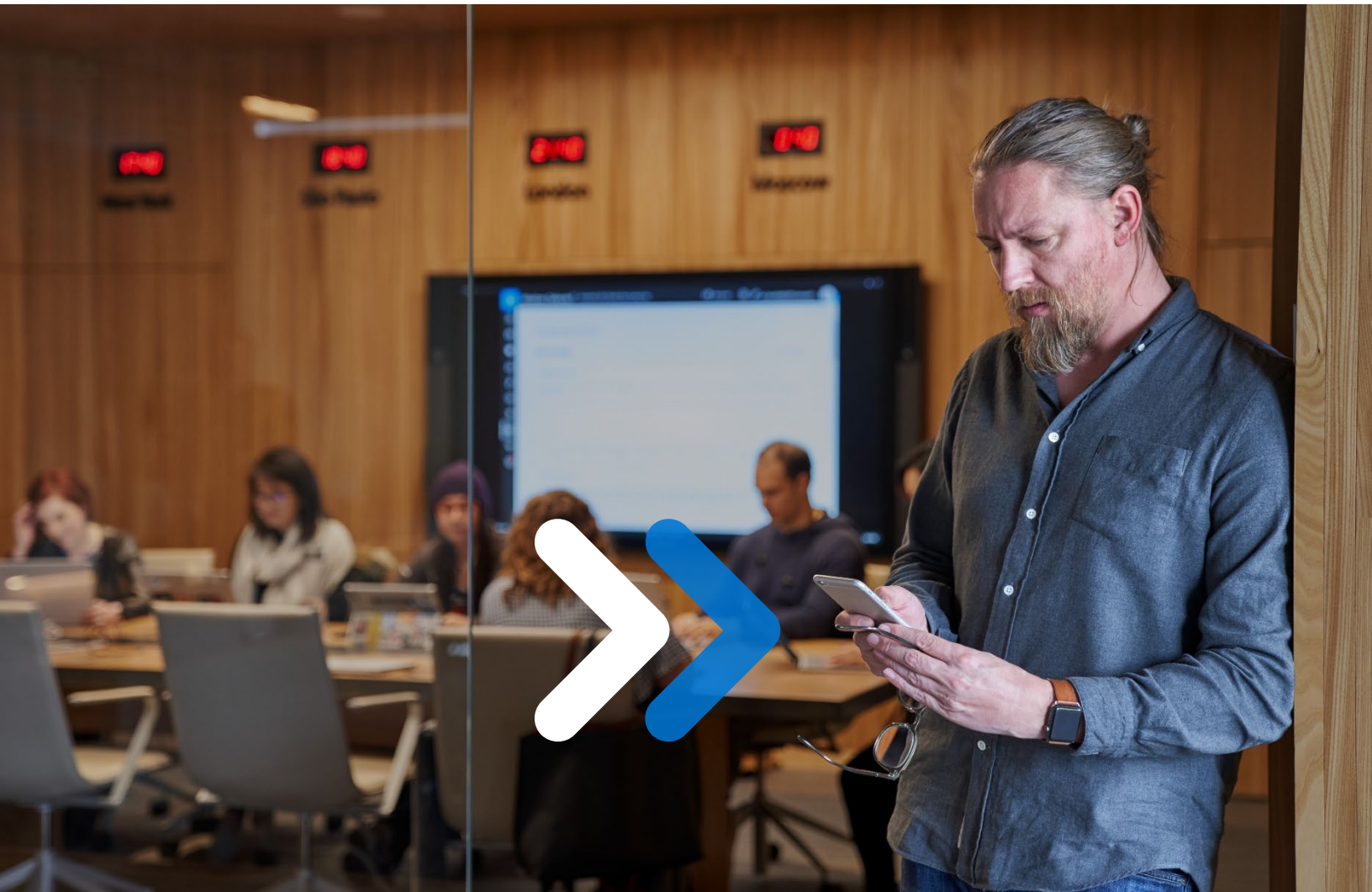



**붙임 11. 향후 2년 동안 제로 트러스트 예산 예상**



## 제로 트러스트 전략의 성공을 입증하면 추가적인 투자를 촉진할 수 있습니다.

제로 트러스트를 전적으로 수용한 조직은 향후 2년 동안 투자를 두 배로 늘릴 것으로 예상하고 있으며, 아직 채택하지 않은 조직은 더 뒤처질 것으로 예상됩니다. 채택하지 않은 조직들은 보안 계획에 제로 트러스트의 우선 순위를 지정하고(42%대 66%), 예산 증가(66%대 72%)에 대해 예상할 때 완전히 구현한 경쟁업체에 뒤처질 뿐만 아니라 향후 IoT 및 OT 보안 관리에 대한 자신감이 매우 낮습니다(40%대 53%).



# 직원과 함께 과제를 극복하는 것이 제로 트러스트 투자를 두 배로 늘리는 열쇠가 될 것입니다.

제로 트러스트 전략 채택이 급속히 발전함에도 불구하고 조직이 전략 구현을 통해 더 발전하려면 무수히 많은 과제를 극복해야 합니다. (붙임 12 참조) 리소스와 리더십 과제는 다음과 같은 범주에서 가장 널리 퍼져 있습니다. 제로 트러스트 전략을 구현하는 데 필요한 시간과 최고 경영진 리더십의 지원 부족이 구현에 대한 가장 큰 장애물이며, 지원 부족은 호주/뉴질랜드(65%)에서 특히 두드러집니다.

또한 조직의 45%가 장애물로 생각하는 예산 제약은 리소스와 리더십 과제에 영향을 미칠 수 있습니다.

예를 들어, SDM의 21%는 제로 트러스트에 대한 투자 ROI를 입증하는 데 어려움을 겪기 때문에 구현의 장애물이 되고 있으며, 이는 최고 경영진의 지원 부족으로 이어질 수 있는 문제입니다. 비미국 시장은 예산 제약이 있을 가능성이 높기 때문에(일본 60%, 독일 57%, 호주/뉴질랜드 57%), 파급 효과로 일본, 독일, 호주/뉴질랜드의 제로 트러스트 전략 구현이 미국에 비해 더 낮고 느려질 수 있습니다.

## 붙임 12. 제로 트러스트의 장애물

| 리소스 문제 60% | 리더십 53% | 기술 46% | 공급업체 46% | 예산 제약 45% |
|---|---|---|---|---|
| 20% 구현하는 데 너무 오래 걸림 | 20% 폭 넓은 최고 경영진 리더십의 지원 부족 | 21% 보안 솔루션 통합의 어려움 | 21% 공급업체의 구현 지원 필요 | 21% 제로 트러스트 전략 구현 비용 |
| 19% 내부 변화 관리 부족 | 19% 이해관계자의 지원 부족 | 19% 레거시 시스템과의 비호환성 | 21% 적합한 공급업체 파악의 어려움 | 21% ROI 입증의 어려움 |
| 18% 더 많은 교육 자료 필요 | 19% 설득력 있는 비즈니스 사례를 만들기 위해 도움이 필요 | 19% 조직 전체로 확장하기 어려움 | 17% 혁신적인 파트너를 찾을 수 없음 | 14% 예산이 충분하지 않음 |
| 17% 조직 규모에 필요하지 않음 | 18% 조직 차원의 지원 부족 | | | |
| 16% 제대로 구현할 수 있는 적절한 인재가 없음 | | | | |

"초기 지원은 어려웠지만 이해관계자로서 프로젝트에 투자하겠다는 합의에 도달하자 모두가 참여했습니다."

미국의 보안 의사 결정자
핀테크

# 보안 의사 결정자는 전체적이거나 통합된 공급업체를 다소 선호합니다.

조직은 제로 트러스트 공급업체 전략과 관련하여 제품군을 최대로 활용하는(best-in-suite) 접근 방식 또는 분야별 공급업체를 선정하는(best-in-breed) 접근 방식을 선택해야 하는 상황에 처해 있습니다. 전자는 전체적이거나 통합된 공급자로부터 제로 트러스트 아키텍처를 위한 제품군을 구입하는 것을 포함하며, SDM은 이 솔루션이 내부적으로 리소스가 부족한 조직에게 더 많은 전문 지식, 리소스 및 단순성을 제공한다고 생각합니다. 그러나 이 접근 방식에서는 취약점 증가와 유연성 부족이 우려됩니다. (붙임 13 참조)

분야별 공급업체를 선정하는 전략은 전문 공급업체로부터 개별 제로 트러스트 기술 구성 요소를 확보하는 것입니다. 제품군 최대로 활용하는 전략과는 달리 다양한 분야의 전문화된 공급업체에 의존하여 더 큰 유연성을 제공하므로 조직의 전략에 보다 밀접하게 부합할 수 있습니다. 즉, 보안 전문가들은 분야별 공급업체 선정이 더 비용이 많이 들고, 자원을 더 많이 필요로 하며, 가시성을 저해한다고 생각하므로 결과적으로 공급업체와 예산 문제가 발생할 수 있습니다. (붙임 14 참조)

조직의 접근 방식이 크게 나뉘지만, 다수의 SDM(55%)은 전체적인(제품군 최대 활용) 공급업체와 협력하는 것을 선호합니다. (그러나 호주/뉴질랜드 조직의 52%는 분야별 공급업체 선정을 선호합니다.)

**붙임 13. 제품군을 최대로 활용하는 접근 방식의 이점 및 장애물 – 상위 2위**

| ⊕ 제품군을 최대로 활용하는 이점 | |
|---|---|
| 공급업체가 솔루션 전반에서 산업별 전문 지식을 보유 | 24% |
| 더 많은 리소스를 이용한 제로 트러스트 전략 계획 | 23% |
| 보안 스택 간소화 | 22% |

| ⊖ 제품군을 최대로 활용하는 단점 | |
|---|---|
| 단일 공급업체에 대한 의존도로 취약점 증가 | 34% |
| 레거시 아키텍처와 더욱 복잡성 높은 통합 필요 | 33% |
| 특수 기능을 위한 유연성 감소 | 29% |

**붙임 14. 분야별 공급업체를 선정하는 접근 방식의 이점 및 장애물 – 상위 2위**

| ⊕ 분야별 공급업체를 선정하는 이점 | |
|---|---|
| 제로 트러스트 전략의 모든 구성 요소에 대해 가장 적합한 솔루션을 추구할 수 있는 유연성 | 33% |
| 조직의 아키텍처 또는 전략과 솔루션을 더욱 긴밀하게 조정 가능 | 30% |
| 다양한 공급업체와의 혁신 기회 증가 | 26% |

| ⊖ 분야별 공급업체를 선정하는 단점 | |
|---|---|
| 비용 증가 | 29% |
| 여러 솔루션에서 데이터 공유가 불가능 | 26% |
| 내부 팀이 채택하고 관리하기에는 많은 솔루션의 양 | 26% |

# 최종 의견

보안 위험이 더 빈번해질 뿐만 아니라 더 부도덕해지면서 시장과 업계 전반의 조직은 제로 트러스트 전략을 채택하여 "신뢰하지 않고 항상 검증"하도록 안내하고 있습니다. 제로 트러스트 전략은 전반적인 보안 태세, 최종 사용자 환경 및 생산성을 개선하고, 직원의 보안 절차를 간소화하며, 비용을 절감하려는 조직에게 최우선 보안 과제입니다. 제로 트러스트 전략의 이점은 잘 자리 잡았지만, 리더십 간의 제한된 자원과 회의론이 보편적인 전략 구현을 방해하고 있습니다.

제로 트러스트 전략의 채택은 코로나19 팬데믹에서 일부 영향을 받으면서 지난 3년 동안 가속화되었습니다. 결정적으로 원격 및 하이브리드 워크플레이스로의 전환으로 제로 트러스트 접근 방식이 광범위하게 채택되고 있으며, 직원들이 조직 외부에서 때때로 개인 디바이스를 통해 액세스하더라도 시스템과 데이터에 대한 보호를 보장합니다. 코로나19로 인해 가속화된 채택은 전체적인 제로 트러스트 준비 태세를 확인하는 좋은 예측 변수이며, 팬데믹 동안 전략을 수용한 조직은 경쟁업체보다 더 많은 보안 위험 영역에서 전략을 구현했습니다.

즉, 가장 발전된 제로 트러스트 전략 채택자조차도 해야 할 일이 남아 있으며, 제로 트러스트 성숙도에 대한 조직의 오해는 조직도 알 수 없는 취약점을 남길 수 있습니다.

시장 전반의 조직 대다수는 제로 트러스트 전략의 중요성이 시간이 지남에 따라 증가할 것이며 차례로 예산도 증가할 것으로 예상합니다. 예상되는 우선 순위 변경은 예산 문제가 채택의 가장 큰 장애물인 미국 이외의 시장에서 특히 중요합니다. 완전한 구현을 위해 노력하는 것은 재정적으로나 논리적으로 매우 큰 부담일 수 있습니다. 제로 트러스트 접근 방식의 이점은 여전히 부정할 수 없으며 Microsoft는 급증하는 변화에 뛰어드는 조직들을 안내하고 지원할 것입니다.

제로 트러스트에 대해 자세히 알아보고 조직의 제로 트러스트 성숙도를 평가하려면 아래 페이지를 참조하세요.

**aka.ms/zerotrust**

# 연구 목표 및 참가자 모집 세부 사항

연구 목표는 다음과 같습니다.

1. 제로 트러스트 접근 방식의 현재 상태 이해
2. 제로 트러스트 접근 방식을 채택하는 사고 방식, 모범 사례, 이점 및 과제 발견
3. 제로 트러스트 접근 방식의 미래 탐색
4. 제로 트러스트 접근 방식의 혁신과 동향 맥락화

보안 의사 결정자는 다음과 선별 기준을 충족해야 했습니다.

사이버 보안, 보안 운영, 위협 방지, ID 관리, 위험 관리, 애플리케이션 보안, 디지털 포렌식 및 사건 대응을 비롯한 조직의 보안에 대한 책임

엔터프라이즈급 기업(미국은 직원 1000명 이상, 독일/일본/호주/뉴질랜드는 직원 500명 이상)에서 정규직으로 재직

25~75세

제로 트러스트에 익숙함

제로 트러스트 전략 개발/구현에 대한 의사 결정에 참여

2021년 4월 일련의 연구 위해 인터뷰한 911명의 보안 의사 결정자 중:

미국, 477명의 SDM 인터뷰

독일, 201명의 SDM 인터뷰

호주/뉴질랜드, 126명의 SDM 인터뷰

일본, 107명의 SDM 인터뷰

*참고: 글로벌 코로나19 팬데믹 동안 변화하는 단계적 확산/봉쇄 단계에서 연구가 수행되었습니다.*