CSO

Microsoft Security

후원 콘텐츠

제로 트러스트 보안:
얼리 어답터에게 얻은 교훈

CSO Microsoft Security

목차

CSO Microsoft Security

소개

지난 2년간의 혼란은 기존의 IT 및 보안 모델을 뒤흔들었습니다. 그 결과 제로 트러스트 보안은 흥미로운 개념에서 최신 엔터프라이즈 보안의 기초로 빠르게 진화했습니다.

Foundry의 새로운 연구에 따르면 조직의 52%는 제로 트러스트 아키텍처를 테스트 중이거나 구축했으며 15%는 제로 트러스트 모델을 연구하고 있습니다. 제로 트러스트를 도입한 조직들은 제로 트러스트 구축이 고객 데이터 보호 개선, 복잡성 감소, 기업 리소스에 대한 안전하고 안정적인 액세스 제공 등 수많은 이점을 제공했다고 보고했습니다.

본 eBook에서는 CISO가 수많은 공격 벡터로 인한 여러 위험으로부터 조직을 보호하는 데 도움이 되는 제로 트러스트 전략의 중요성을 강조하는 Foundry 연구 결과를 살펴봅니다. 본 eBook은 제로 트러스트 여정을 시작하는 조직들을 위해 제로 트러스트 구현 방법에 대한 지침도 제공합니다.

설문 조사 관련 정보

Foundry는 2022년 2월과 3월에 미국 기업을 대상으로 제로 트러스트 도입의 현황을 조사했습니다. 응답자는 직원이 500명 이상인 회사의 IT 매니저 이상의 직급으로 사이버 보안 제품 및 서비스 구매와 관련한 역할을 담당하는 사람으로 한정되었습니다.

문항 수는 23개였으며 총 응답자 수는 250명이었습니다.

CSO Microsoft Security

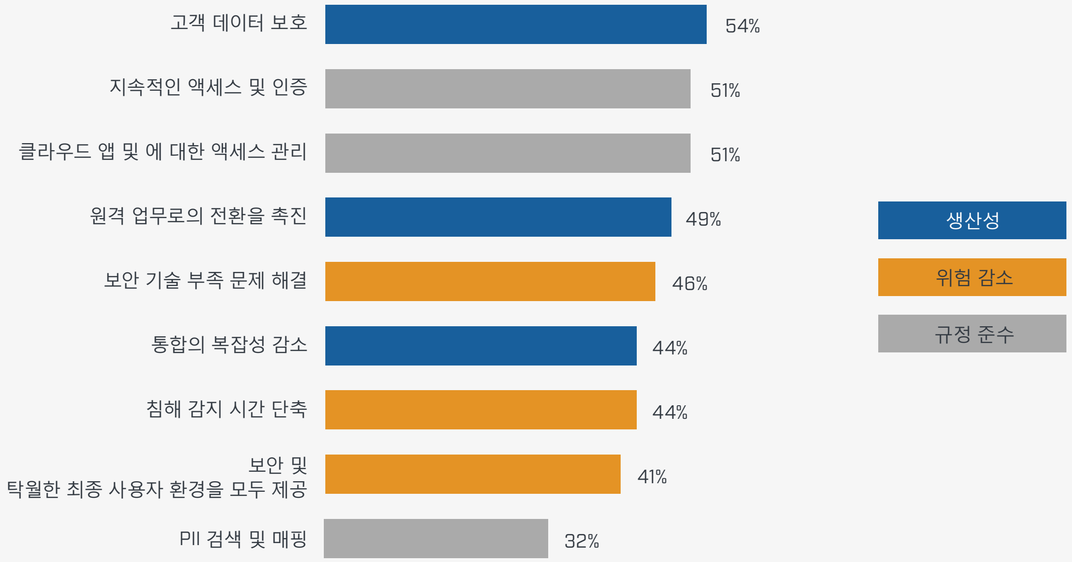
실질적인 활용에서 가치를 제공하는 제로 트러스트

설문 조사 결과와 IT 및 보안 경영진과의 심층 인터뷰에 따르면 대부분의 조직에서 제로 트러스트를 가장 중요하게 여기는 것으로 나타납니다. 제로 트러스트의 다양한 구성 요소를 구축한 조직들은 이미 제로 트러스트의 이점을 체감하고 있습니다.

제로 트러스트를 구현한 대부분의 응답자(87%)는 아키텍처가 구현, 도입 및 통합에 대한 원래 목표 이상을 달성하고 있다고 밝혔습니다.

한 글로벌 소매업체의 IT 담당자 "(제로 트러스트는) 표준 운영 절차로 자리잡았습니다. 예전으로 돌아갈 수는 없을 것 같습니다."라고 전했습니다. (응답자들은 보안 계획에 대해 자유롭게 이야기하는 대신 익명 처리되었습니다.)

제로 트러스트 구현 이후 확보된 이점



12%의 응답자가 상기 *모든* 이점을 누리고 있다고 응답

출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 250명

CSO Microsoft Security

응답자의 약 44%는 제로 트러스트가 통합 보안 아키텍처 구현에 내재된 복잡성을 줄였다고 보고했습니다. 직원 수가 3,500명인 콜센터 회사의 CISO는 "프레임워크를 다루고 프레임워크를 통해 작업하기 때문에 일의 복잡성이 줄어듭니다."라고 전했습니다.

직원이 17,000명인 금융 서비스 회사의 부사장 겸 CISO는 제로 트러스트의 일환으로 구현한 다중 인증이 직원들에게 좋은 반응을 얻었다고 응답했습니다. CISO는 "실제로 직원 만족도가 높아졌습니다. 이제 회사에서 제공한 컴퓨터를 사용하거나 VPN 클라이언트를 사용하지 않고도 어디에서나 리소스에 접근할 수 있습니다."라고 설명했습니다.

CISO는 최소 권한 액세스라는 개념 또한 큰 이점을 제공했다고 언급했습니다. 이와 관련하여 CISO는 "권한 액세스 시스템을 구현한 덕분에 시스템 관리자의 치명적인 오류가 줄어들었습니다."라며 "시스템 관리자는 특정한 작업과 특정 기간에 대한 권한을 얻기 때문에 실수할 가능성이 적습니다."라고 전했습니다.

소매 회사의 IT 담당자는 피싱 및 기타 사이버 공격이 증가하는 상황에서 제로 트러스트의 이점과 관련하여 "이러한 유형의 도구가 없었다면 아마 지금 좋지 않은 상황에 처해 누군가에게 비트코인을 지불했을 것입니다."라고 전했습니다.

CSO Microsoft Security

제로 트러스트 구축의 추진 요인

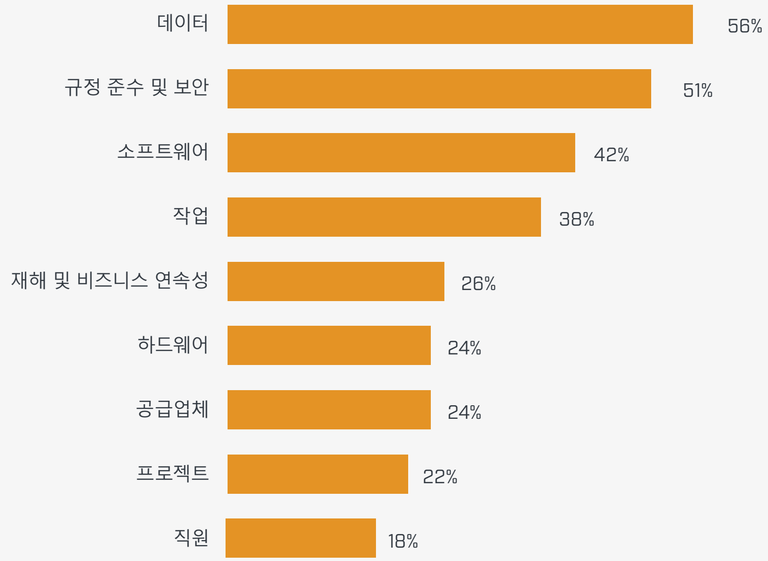
기업들은 사건들이 복합적으로 발생하면서 제로 트러스트 아키텍처를 최소한 고려는 하게 되었습니다. 가장 중요한 것은 수많은 위협에 대응하여 여러 리소스에 대한 위험을 관리해야 한다는 점입니다. 설문 조사 응답자들은 수년간 발생한 보안 사고가 제3자인 개인 또는 조직의 보안 취약성 등 수많은 원인에서 비롯되었다고 응답했습니다. 기타 원인에는 다음이 포함됩니다.

- 예상치 못한 비즈니스 위험
- 서비스 또는 시스템의 구성 오류
- 악의적인 국제적 내부자 공격
- 비악의적인 사용자 오류(예: 피싱 피해자)
- 손상된 신원
- 패치되지 않은 소프트웨어
- 도난된 개인 인증 정보

이러한 사고는 데이터 등과 관련된 여러 가지 위험을 야기합니다.

많은 조직에서 팬데믹으로 인해 갑작스럽게 원격 근무로 전환하면서 기존의 경계 기반 보안 모델을 더 이상 사용되지 않게 되었고 이에 따라 제로 트러스트 도입 계획이 가속화되었습니다. 많은 조직들이 더 많은 애플리케이션과 IT 인프라를 클라우드로 이전함에 따라 이미 제로 트러스트 여정을 시작한 상태였지만 팬데믹이 이러한 여정을 촉진하는 추가적인 원인으로 작용한 것입니다.

사이버 보안 위협의 위험에 처한 상위 카테고리



출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 250명

CSO Microsoft Security

예를 들어, 직원 수가 1,700명인 의료 기술 회사의 CISO는 클라우드와 팬데믹으로 인해 어떠한 워크플레이스 모델에도 안전한 기반을 제공할 수 있는 제로 트러스트를 도입하게 되었다고 밝혔습니다.

CISO는 "비즈니스 동인은 당사가 클라우드 기반 회사이며 회사 환경을 보호할 수 있어야 한다는 사실이었습니다."라며 "또한 당사는 팬데믹 기간 동안 유능한 원격 인력을 제공해야 했습니다. (제로 트러스트 덕분에) 당사는 물리적 업무 공간을 대폭 줄일 수 있었고 업무의 최소 60%를 가상 원격 방식으로 유지할 전망입니다."라고 전했습니다.

CSO Microsoft Security

현존하는 위협

또한 규정 준수 요구 사항은 보다 강력한 보안 모델에 대한 필요를 제공했습니다. 직원이 290,000명인 금융 서비스 회사의 글로벌 정보 보안 SVP는 "규제 당국은 당사를 주시하고 있으며 당사가 보안 프레임워크를 계속 개선할 것으로 기대합니다."라고 전했습니다.

일부 조직은 침해라는 바람직하지 않은 이유로 이목을 끌고 관심이 집중되는 상황을 피하기 위해 제로 트러스트 도입을 위한 선제적인 조치를 취했습니다. 직원 수가 3,500명인 고등 교육 기관의 CIO는 "선제적으로 대응하고 대처하고 문제를 방지하려고 노력했습니다."라며 "당사 규모의 기타 지역 기관 기관들은 실제로 침해 문제를 겪으면서 오랫동안 분위기가 침체되기도 했습니다."라고 전했습니다.

이미 심각한 사이버 보안 사고를 경험하면서 보안 전략을 재빨리 재검토하게 된 조직들도 있습니다. 직원 수가 6,000명인 한 보험사는 랜섬웨어 공격을 받아 2주 동안 기업 네트워크가 차단되자 CEO가 직접 제로 트러스트를 도입하라고 주문했습니다. 회사의 IT 개발 부사장은 "당사는 구현에 박차를 가했습니다."라며 "초기에는 확실히 모범 사례였고 랜섬웨어 공격 이후에는 구현이 대폭 가속화되었습니다."라고 전했습니다.

클라우드 기반의 촉매제

주요 금융 서비스 회사의 부사장 겸 CISO는 몇 년 전 팀에서 더 많은 클라우드 기반 리소스를 도입하기 시작하고 사용자가 더욱 모바일화되면서 새로운 보안 아키텍처의 필요성을 인식하게 되었다고 전했습니다.

부사장 겸 CISO는 "과거에 의존했던 전통적인 보안 아키텍처가 앞으로는 공격자로부터 우리를 보호할 수 없다는 것을 깨달았습니다."라고 전했습니다.

이러한 현실은 2020년 초, 전년도에 발생한 공격에서 공격자가 감지되지 않고 경계망에 침투하여 환경 내에서 측면 이동했음을 발견했을 때 더욱 분명히 인식되었습니다. 부사장 겸 CISO는 "당사는 리소스가 존재하는 모든 위치에서 리소스의 사용을 보호 및 인증할 수 있는 새로운 아키텍처가 필요했는데, 제로 트러스트가 바로 이를 위해 설계된 아키텍처였습니다."라고 전했습니다.

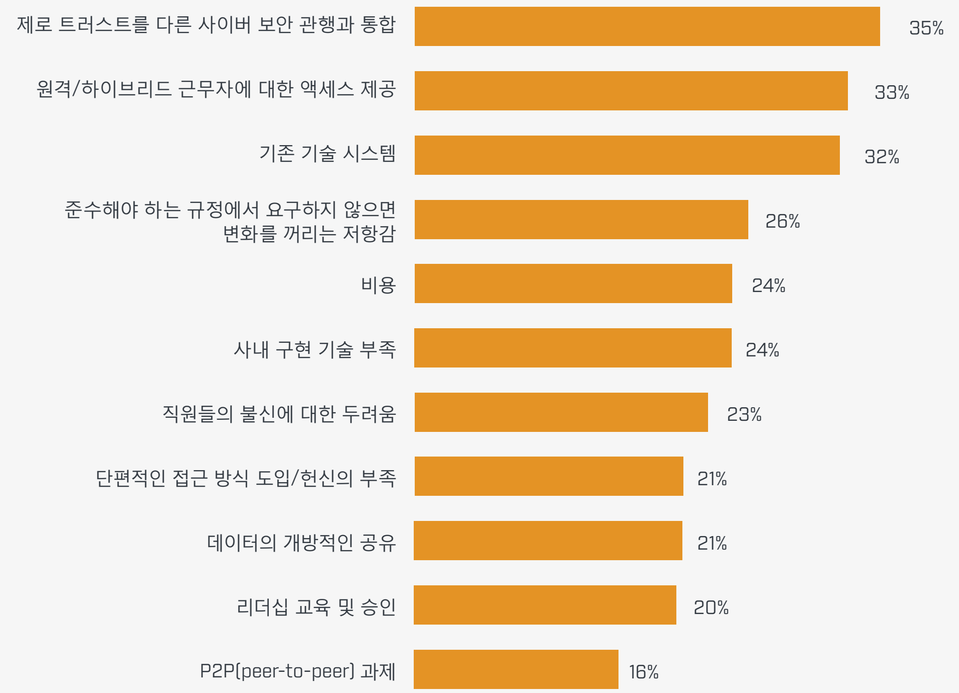
CSO Microsoft Security

제로 트러스트 도입을 위해 극복해야 할 방해 요소

많은 조직에서 제로 트러스트는 보안 구조, 프로세스 및 사고 방식의 근본적인 변화를 의미합니다. 여기에서 제로 트러스트를 도입하기 위해 극복해야 하는 몇 가지 방해 요소를 알 수 있습니다.

CISO는 "조직 내에서 많고 다양한 사일로에 직면하기 시작했습니다."라며 서버, 네트워크 및 데이터베이스 팀이 각각 고유한 웹 서버 및 도구를 보유하고 있었다고 설명했습니다. 그는 "이러한 사일로로 인해 방향성, 작업 방식에 대한 생각이 모두 달랐고 교착 상태에 빠지기 쉬웠습니다."라고 덧붙였습니다.

제로 트러스트 채택을 저해하는 요소



출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 250명

CSO Microsoft Security

Microsoft의 제로 트러스트 제품 마케팅 수석 관리자인 Anthony Mocny에 따르면 이러한 문제를 발견하는 것은 실제로 제로 트러스트의 긍정적인 부작용이 될 수 있습니다. Anthony Mocny는 "제로 트러스트는 아키텍처로서 여러 기술 분야 내에 존재하는 보안 팀의 사일로를 해체하고 팀이 긴밀하게 연결되어 함께 작업할 수 있도록 설계되었습니다. 이는 팀의 협력 측면에서 문화적 변화를 의미할 수도 있습니다."라고 전했습니다.

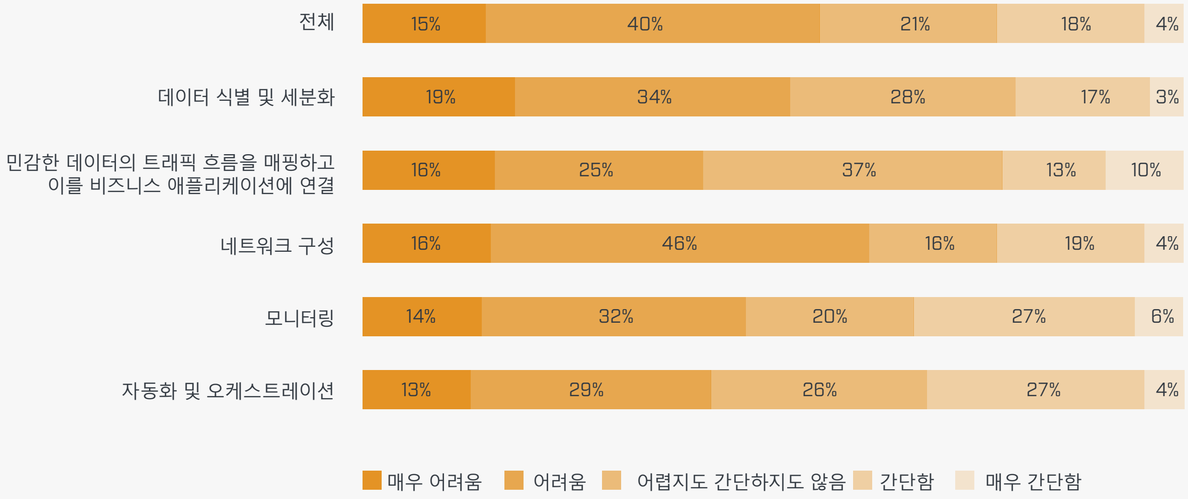
금융 서비스 부사장 겸 CISO에게 기존 애플리케이션은 제로 트러스트 도입을 준비하는 과정에서 극복해야 할 방해 요소였습니다. 부사장 겸 CISO는 "기존 애플리케이션에 최신 인증 기술을 적용해야 했습니다. 애플리케이션이 얼마나 오래되었는지에 따라 어려운 작업이 될 수도 있죠."라고 전했습니다.

CSO Microsoft Security

구축 관련 과제

기업이 제로 트러스트 여정을 시작하면 다양한 구현 문제가 나타날 수 있습니다. 설문 조사 응답자의 절반 이상(56%)은 제로 트러스트 구현이 어렵거나 매우 어렵다고 응답했습니다. 자세한 응답 내용은 다음과 같습니다.

제로 트러스트 구현은 얼마나 어려운가?



출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 168명

세분화 및 마이크로 세분화와 관련된 문제는 심층 인터뷰에서 자주 언급되었습니다.

금융 서비스 기업의 부사장 겸 CISO는 "네트워크를 개별 호스트로 세분화하는 것은 내부 네트워크의 모든 단일 호스트 사이에 작은 방화벽을 설치함으로써 모든 트래픽을 확인하고 개별 기계까지 제어할 수 있게 되는 작업입니다. 이러한 세분화는 보안 측면에서 엄청난 이점을 제공하지만, 사실상 수만 개의 방화벽을 관리해야 하기 때문에 구현하기가 매우 어렵습니다."라고 설명했습니다.

트래픽 흐름 매핑 프로세스 또한 수개월이 소요될 수 있습니다. 직원 수가 5,000명인 출판 및 미디어 회사의 CTO는 보호해야 하는 중요한 데이터, 애플리케이션 및 네트워크 서비스를 정의한 후 "네트워크를 따라 트랜잭션 흐름을 매핑하고 이를 정보 그룹으로 파악하고자 했습니다. "(그러고 나서) 해당 정보의 부분과 이러한 정보가 실제로 네트워크를 이동하는 방법을 정보의 단일 패킷에 이르기까지 세분화했습니다."라고 전했습니다. 이 시점에서 회사는 각 유형의 트래픽 흐름에 제로 트러스트 정책을 적용했습니다. CTO는 "당사 네트워크를 모니터링하고 유지하는 새로운 역량을 강화하기도 했습니다."라고 전했습니다.

이러한 과제에도 불구하고 많은 응답자는 제로 트러스트가 궁극적으로 일상적인 운영을 단순화한다고 응답했습니다. 글로벌 정보 보안 금융 서비스 업체의 SVP는 기존 기술을 사용하면 "변경에 며칠이 소요됩니다. 또한 변경 사항을 모든 하드웨어 및 소프트웨어 구성 요소에 적용해야 하며 여기에 많은 리소스가 사용되고 있습니다."라고 전했습니다. SVP는 "제로 트러스트는 장기적으로 아키텍처 복잡성을 최소화하고 동일한 유형의 작업을 수행하는 데 필요한 직원 수를 줄이는 것으로 판단됩니다."라고 덧붙였습니다.

CSO Microsoft Security

제로 트러스트 구현 모범 사례

더 많은 기업에서 제로 트러스트 아키텍처를 구현함에 따라 다른 기업에서 참고할 수 있는 로드맵과 모범 사례가 개발되고 있습니다. 다음은 배포를 계획할 때 고려해야 할 5가지 사항입니다.

시작부터 무리하지 않을 것

네트워크, 데이터, 애플리케이션, ID, 엔드포인트 및 인프라 전반에서 정책 및 보호 수준을 변경해야 하는 광범위한 맥락에서만 제로 트러스트 전략을 수립하려고 한다면 무리가 될 수 있습니다. 고등 교육 업체의 CIO는 "처음에는 제로 트러트스라는 거대한 산을 바라보기만 했고 우리가 정말로 이 산을 오르게 될 것인지에 대해 의문을 품었습니다. 한 번에 한 걸음씩 내딛어야만 시작할 수 있습니다."라고 전했습니다.

CIO와 CIO의 팀은 결국 별도의 네트워크에서 재무 및 급여 응용 프로그램 세분화를 우선시하는 "돈의 흐름을 따라가는" 접근 방식을 도입했습니다.

Mocny에 따르면 보호해야 할 가장 중요한 자산을 식별하는 것이 합리적인 접근 방식입니다. Mocny는 "처음부터 제로 트러스트를 구현하는 이유를 염두에 두어야 합니다."라고 전했습니다.

의심이 될 때는 다중 인증으로 시작할 것

많은 CISO 및 보안 공급 업체들은 보안 스택의 우선 순위를 정할 때 초기에 인증 및 기타 ID 기반 보호에 중점을 둘 것을 권장합니다. Mocny는 "어디에서 시작할지 모르겠다면 다중 인증부터 시작하는 것도 좋습니다."라고 전했습니다.

Microsoft는 다단계 인증이 ID 기반 공격의 90% 이상을 방지할 수 있다고 추정합니다.

금융 서비스 업체 부사장 겸 CISO 또한 이에 동의했습니다. "인증은 제로 트러스트 아키텍처 구현의 기본 요소입니다. 최종 사용자의 신원을 확인할 수 없으면 다른 구성 요소가 작동하지 않으므로 당사 역시 인증에서부터 시작했습니다."

다음으로 금융 서비스 업체의 부사장 겸 CISO는 원격 근무자를 지원하는 데 즉각적인 이점을 제공하는 네트워킹 구성 요소를 다루었습니다. 팀은 기업에서 쉽게 확인할 수 없다는 이유로 여정의 후반까지 마이크로 세분화에 착수하지 않았습니다. 부사장 겸 CISO는 "마이크로 세분화를 완료하면 보안성이 대폭 개선되지만 아무도 차이를 알아차리지 못합니다."라고 설명했습니다.

CSO Microsoft Security

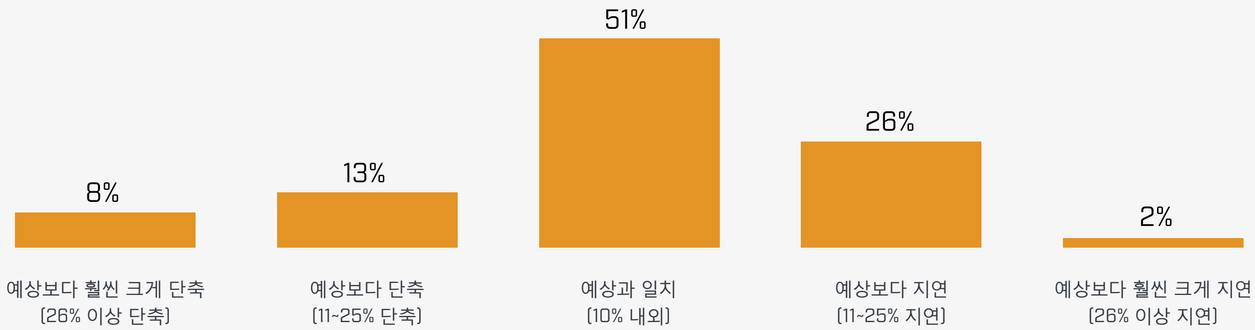
일정을 현실적으로 고려할 것

CISO는 제로 트러스트 배포에 대한 현실적인 기대치를 설정해야 합니다. 금융 서비스 업체의 부사장 겸 CISO는 "제로 트러스트 아키텍처를 구현하는 것은 프로젝트가 아니라 프로그램이고 큰 변화를 야기합니다."라며 제로 트러스트 아키텍처 구현은 수많은 프로젝트를 수반하는 데다가 몇 년 동안 지속될 수 있기 때문에 빠르고 쉽게 완료할 수 있는 방법은 없습니다."라고 전했습니다.

부사장 겸 CISO의 동료인 금융 SVP 또한 이에 동의했습니다. 그는 "항상 새로운 기술이 개발되고, 항상 새로운 맬웨어가 등장하고, 항상 새로운 위협이 발생하기 때문에 아키텍처 구현이 완료될 거싱라고 생각하지 않습니다."라고 설명했습니다.

설문 조사 응답자의 대다수(72%)는 배포 일정이 계획대로 진행 중이거나 계획보다 앞서 진행되고 있다고 응답했으며 나머지는 구현 시간이 예상보다 더 오래 걸린다고 응답했습니다.

제로 트러스트가 일정 목표를 충족하는가?



출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 168명

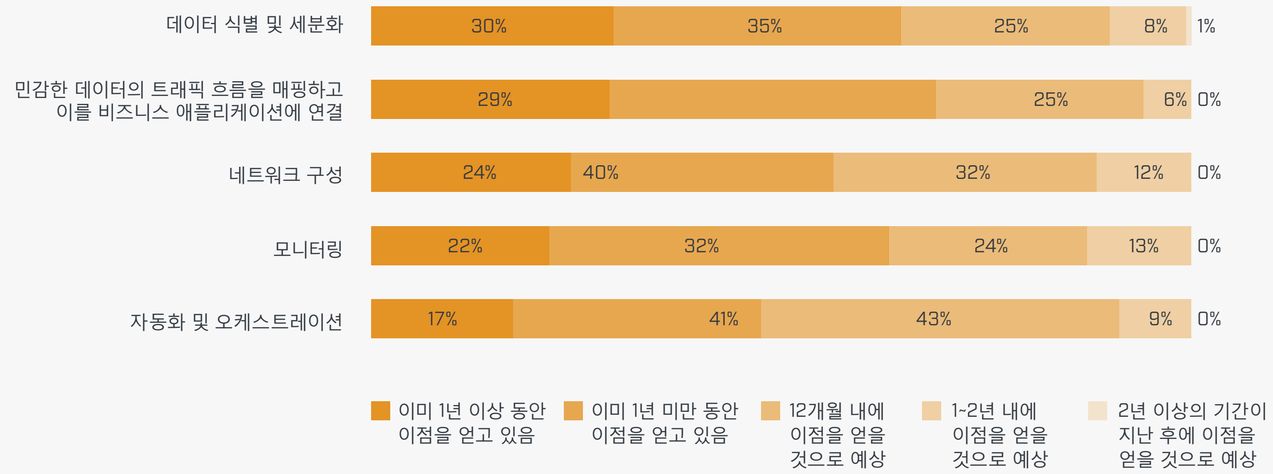
CSO Microsoft Security

진행 과정을 측정할 것

CISO는 제로 트러스트 배포가 진행되는 동안 진행 상황을 측정하는 과정에서 중요 단계에 대한 일정표를 만들 수 있고 만들어야 합니다. 설문 조사 응답자의 약 3분의 2는 데이터 식별 및 분류, 트래픽 흐름 매핑, 네트워크 구성 증 핵심 활동 전반에 걸쳐 1년 이내에 프로젝트 대부분의 측면에서 이점을 얻고 있으며 약 4분의 1 이상은 12개월 이내에 이점을 얻을 것으로 예상한다고 응답하는 등 긍정적인 반응을 보였습니다.

Mocny는 "특징이 계속 변화하는 공격에 맞서 방어해야 하는 상황에서 제로 트러스트는 지속적인 평가가 이루어지기 때문에 여정이라고 할 수 있습니다."라고 전했습니다. "언제나 개선해야 할 점을 찾아야 합니다."

제로 트러스트 이점을 확보하기 위한 일정



출처: 2022년 3월 Foundry 제로 트러스트 도입 설문 조사 응답자 수: 103명

기술 외에 사람에게도 집중할 것

제로 트러스트 보안 모델은 범위가 넓기 때문에 이를 배포하는 IT 및 보안 팀을 포함한 모든 직원에게 영향을 미칩니다. 따라서 대규모 기술 프로젝트와 마찬가지로 원활하고 성공적인 개시를 위해 배포가 새로운 프로세스 및 변경 관리 관행에 부합하도록 하는 것이 중요합니다.

Mocny는 "기술뿐 아니라 문화도 변화합니다. "네트워크 설계자 또는 ID 전문가를 비롯하여 보안을 다루는 팀이 여러 개인 경우 해당 팀이 함께 작업하는 방식도 변경해야 합니다. 모든 기술이 긴밀하게 연결되어 작동하도록 사일로를 해체해야 합니다."라고 전했습니다.

사일로를 제거하려면 시험 및 PoC 프로젝트에 밀접하게 관련된 모든 분야에 걸쳐 팀을 구성해야 합니다. 직원 수가 약 2,000명인 통신 회사의 IT 시스템 담당자는 인증할 수 없으며 갑자기 "신뢰할 수 없는" 서비스로서 시스템을 사용할 수 없게 만드는 서비스를 비롯하여 배포 과정에서 발생한 여러 개의 단일 장애 지점을 해결하느라 애를 쓰고 난 뒤 이러한 교훈을 얻었습니다.

그는 "하나의 서비스를 배포하는 것은 도미노 효과를 일으키고 다른 서비스를 붕괴시킬 수 있습니다. 따라서 배포하기 전에 더 많은 PoC 시간을 갖고, 더 많이 검토하며, 주제 전문가와 더 많은 아키텍처를 검토하는 등 훨씬 더 주의를 기울이고 있습니다."라고 전했습니다.

제로 트러스트 ROI

2021년 **Forrester Consulting Total Economic Impact™** 는 Microsoft Zero Trust 솔루션의 비용 절감 및 비즈니스 이점을 수량화했습니다. Forrester가 인터뷰한 5개 기업에 따르면 한 복합 조직은 Microsoft를 통해 제로 트러스트 아키텍처를 구현하여 3년 동안 92%의 투자 수익을 실현했습니다.

이 복합 조직은 또한 엔드포인트 관리, 바이러스 백신 및 맬웨어 방지 솔루션을 포함하여 제로 트러스트에서 중복되는 보안 도구의 필요성을 없애 직원당 월 평균 20달러를 절감했습니다.

CSO Microsoft Security

제로 트러스트 여정 중 현재 위치

설문 조사에서 알 수 있듯이 제로 트러스트 보안 모델의 이점은 CISO와 보안 팀이 직면한 일부 배포 과제를 넘어섭니다. 세심한 계획을 통해 이러한 과제를 극복하면 조직에서 신속하게 보호 수준을 개선하고 위험을 줄이며 비즈니스 전반에서 가치를 제공할 수 있습니다.

조직의 제로 트러스트 성숙도를 평가하고 보다 실용적인 배포 리소스를 확인하려면 Microsoft의 **제로 트러스트 성숙도 모델 평가**를 활용해 보시기 바랍니다.