백서

제로 트러스트, 사이버 보안 전략의 우선순위

작성자: John Grady, Enterprise Strategy Group 수석 애널리스트

2023년 1월

Enterprise Strategy Group 백서는 Akamai의 의뢰를 받아 TechTarget, Inc.의 라이선스 하에 배포되었습니다.

목차

요약 보고서

사이버 보안과 관련해 불편하지만 반드시 인정하고 넘어가야 하는 중요한 사실이 있습니다. 너무나 많은 기업이 시스템, 네트워크, 정책 및 실무에서 벌어지는 상황을 암묵적으로 신뢰하고 있습니다. 사이버 보안에서 암묵적으로 신뢰할 수 있는 영역이란 없으며, 기업에는 다양하면서도 심층적인 리스크가 내재되어 있습니다.

제로 트러스트는 10년 이상의 기간을 거쳐 사이버 보안의 주요 관행으로 발전했으며, 지금은 기업의 사이버 보안 방어 프레임워크에서 중요한 전략적 요소이자 핵심으로 널리 활용되고 있습니다.

제로 트러스트가 점점 더 정교한 형태로 증가하는 위협을 차단하기 위한 기업 역량의 핵심으로 자리 잡게 된 것은 단순히 스마트 기술 관행 덕분이 아니라, 스마트 비즈니스 때문에 가능했습니다. 비즈니스 기능에 필요한 사용자에게만 접속 권한을 제한함으로써 위협의 영향을 차단하는 것이 새로운 모범 사례가 되었습니다. 이 모범 사례를 실천함으로써 기업은 시스템 침투, 멀웨어 또는 랜섬웨어 배포, 데이터 유출에 이르는 다양한 유형의 공격을 차단할 수 있습니다.

제로 트러스트는 잠재적인 위협에 대한 차단막을 구축해 유출 발생 시 기업의 피해를 최소화함으로써 디지털 자산을 보다 스마트하게 효율적으로 그리고 효과적으로 보호할 수 있습니다.

오늘날 기업의 복잡성 문제

비즈니스 차별화 요소로 기술을 앞세우는 소규모 기업을 포함해 거의 모든 기업이 부담스러우면서도 까다로운 사이버 보안 환경에 직면했습니다. 공격 건수가 증가하면서 공격과 관련된 경제, 규제, 법률, 운영 및 브랜드의 부담 비용도 증가하고 있습니다.

사이버 보안 방어는 더욱 정교하고 지속적인 공격자 그룹에 대응할 수 있도록 최신화되어야 하며, 공격자들은 더 정확하게, 더 빠르고 더 빈번하게 공격을 감행하기 위해 인공지능 및 머신러닝과 같은 기술을 사용하고 서로 공조하며 각자의 지식을 이용하고 있습니다. 기업은 끈질긴 공격자들과 이들의 혁신에 대해 더 큰 경각심을 갖게 됐지만, 인프라, 아키텍처, 데이터 모델 및 디지털 비즈니스 관행이 점점 더 복잡해지는 만큼 사이버 보안 전략을 한층 강화할 필요가 있습니다.

최신 사이버 보안 전략의 핵심은 이처럼 증가하는 디지털 복잡성을 이해하고 이에 대한 계획을 수립하는 것입니다. 복잡성이 증가하는 이유로 다음과 같은 여러 가지가 있습니다.

- 온프레미스와 클라우드 애플리케이션이 동시에 급속히 확산되면서 데이터는 물론, 공격 대상과 함께 잠재적 네트워크 진입점도 늘었습니다.
- 디바이스 및 데이터 소스의 확장 역시 가속화되면서, 공격 기법과 사이버 범죄자가 이용할 수 있는 새로운 진입점이 확대되고 있습니다. 여기에는 기업의 물리적 시설 외부에 존재하는 네트워크에서 접속 가능한, 관리되지 않고 보호되지 않는 개인 디바이스 또는 보안 정책으로 제대로 제어되지 않는 네트워크 연결 디바이스가 포함될 수 있습니다.
- 원격 근무 및 하이브리드 근무로 빠르게 전환되는 추세와 함께 SaaS 애플리케이션, 가정에서 구입해 사용하는 클라우드 서비스, 잠재적인 '악성 IT'가 급격히 증가하면서 보안의 복잡성은 더욱 심화되었습니다.

기업에서 클라우드 도입이 늘고 있다는 점도 복잡성을 가중시킨 중대한 사유입니다. 클라우드는 분명 대부분의 기업에서 IT 전략의 중요한 일부이자 최신 IT 아키텍처의 핵심으로 널리 활용되고 있습니다. 멀티 클라우드 및 하이브리드 클라우드는 대부분의 기업에서 표준이 되었으며, 많은 기업이 클라우드 퍼스트 또는 클라우드 네이티브 원칙을 도입하고 있습니다. 그러나 기업들은 아직 클라우드 보안에 적절한 주의를 기울이지 않고 있으며, 사이버 공격자의 새로운 침입 경로는 점점 늘어나고 있습니다.

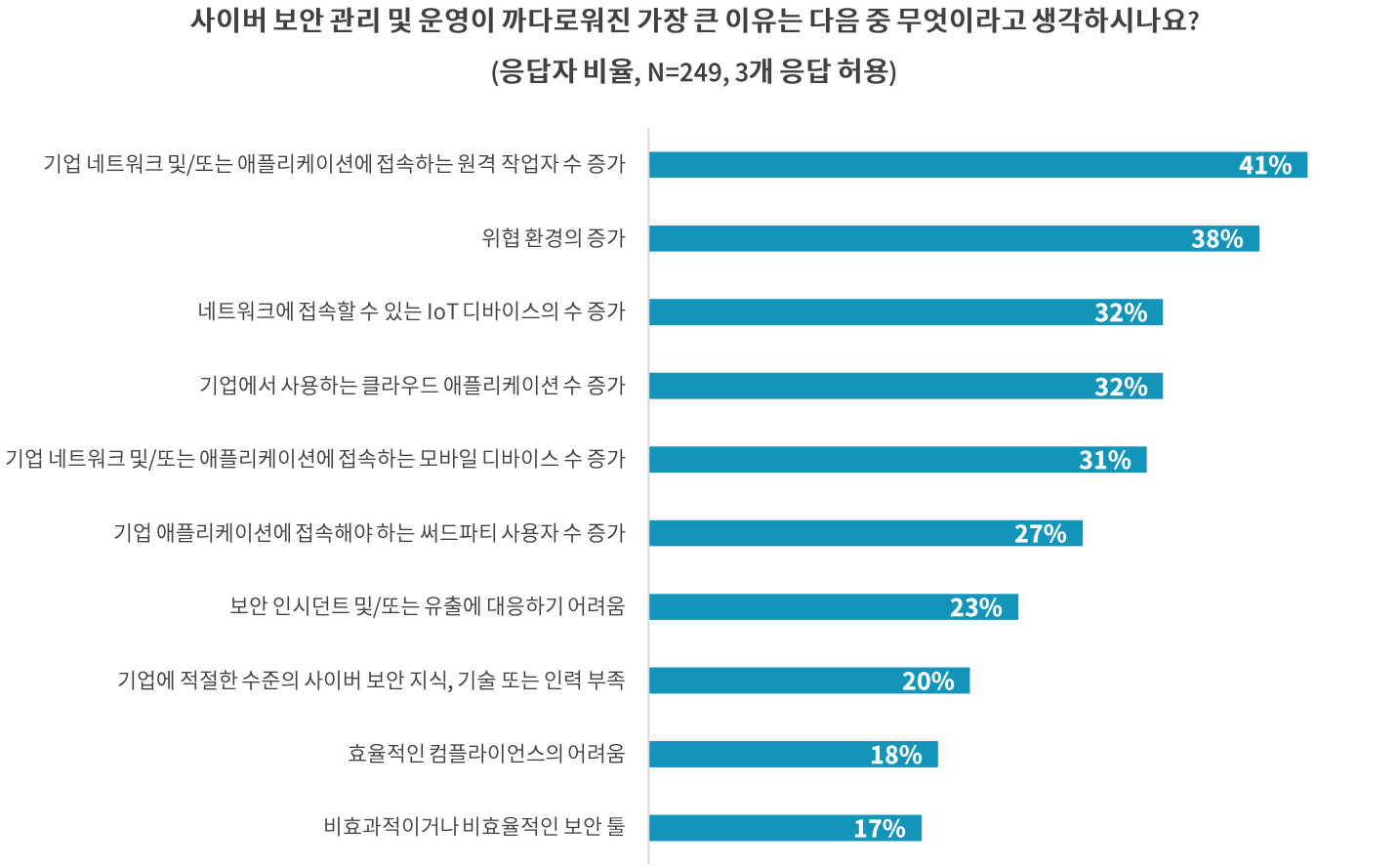
결과적으로 데이터, 애플리케이션, ID, 자격 증명 및 지적 재산을 효율적으로 완벽하게 보호하는 것이 그 어느 때보다 어려워졌습니다. 기존의 보안 접근 방식은 대부분 온프레미스 인프라 접근 방식이 지배적이고, 디바이스 수와 유형이 제한적이던 시절에 맞게 설계되었기 때문에 최근 추세를 따라올 수 없습니다.

위험성도 더 높아졌습니다. 데이터 유출로 인한 비용은 매년 증가하고 있으며, 미흡한 보안으로 발생하는 규제 및 거버넌스 관련 문제도 지속적으로 더 큰 부담이 되고 있습니다.

그 결과 사이버 보안은 점점 더 까다로워지고 있으며, 완전하고 적절한 사이버 보안 체계를 구축하기가 더욱 어려워졌습니다. TechTarget의 ESG(Enterprise Strategy Group) 연구에 따르면, 59%의 기업이 지난 2년 동안 사이버 보안이 더욱 까다로워졌다는 사실에 동의했습니다. 가장 많이 언급된 두 가지 이유는 기업 네트워크 및/또는 애플리케이션에 접속하는 원격 작업자 수의 증가(41%)와 위협 환경 증가(38%, 그림 1 참조)입니다. ESG 연구에 따르면, 네트워크에 접속하는 사물 인터넷(IoT) 디바이스의 증가(32%), 조직에서 사용하는 클라우드 애플리케이션의 증가(32%), 그리고 네트워크 및/또는 애플리케이션에 접속하는 데 사용되는 모바일 디바이스의 지속적인 증가(31%)와 같은 기타 리스크 요소도 가까운 미래에 더욱 증가할 것으로 보입니다.[1]

[1] 출처: Enterprise Strategy Group 설문조사 결과, *The State of Zero Trust Security Strategies,* 2021년 5월. 이 백서에 포함된 모든 Enterprise Strategy Group 연구 참고 자료 및 차트는 이 설문조사 결과 세트에서 발췌한 것입니다.

그림 1: 사이버 보안이 더욱 까다로워진 이유



출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

기업은 여기에서 언급된 이유를 포함해 기타 복잡성과 리스크 요소를 파악하고 전체 사이버 보안 전략에서 제로 트러스트의 우선순위를 높이는 데 적극적으로 임해야 합니다. 제로 트러스트가 이러한 리스크를 완벽하게 제거하지는 못하지만, 기업이 디지털 자산을 보호하고 사이버 위생을 현대화할 수 있도록 더욱 강력하고 안전한 기반을 구축하는 데 도움이 될 것입니다.

추진력을 얻고 있는 제로 트러스트, 그러나 여전히 남아 있는 주요 과제

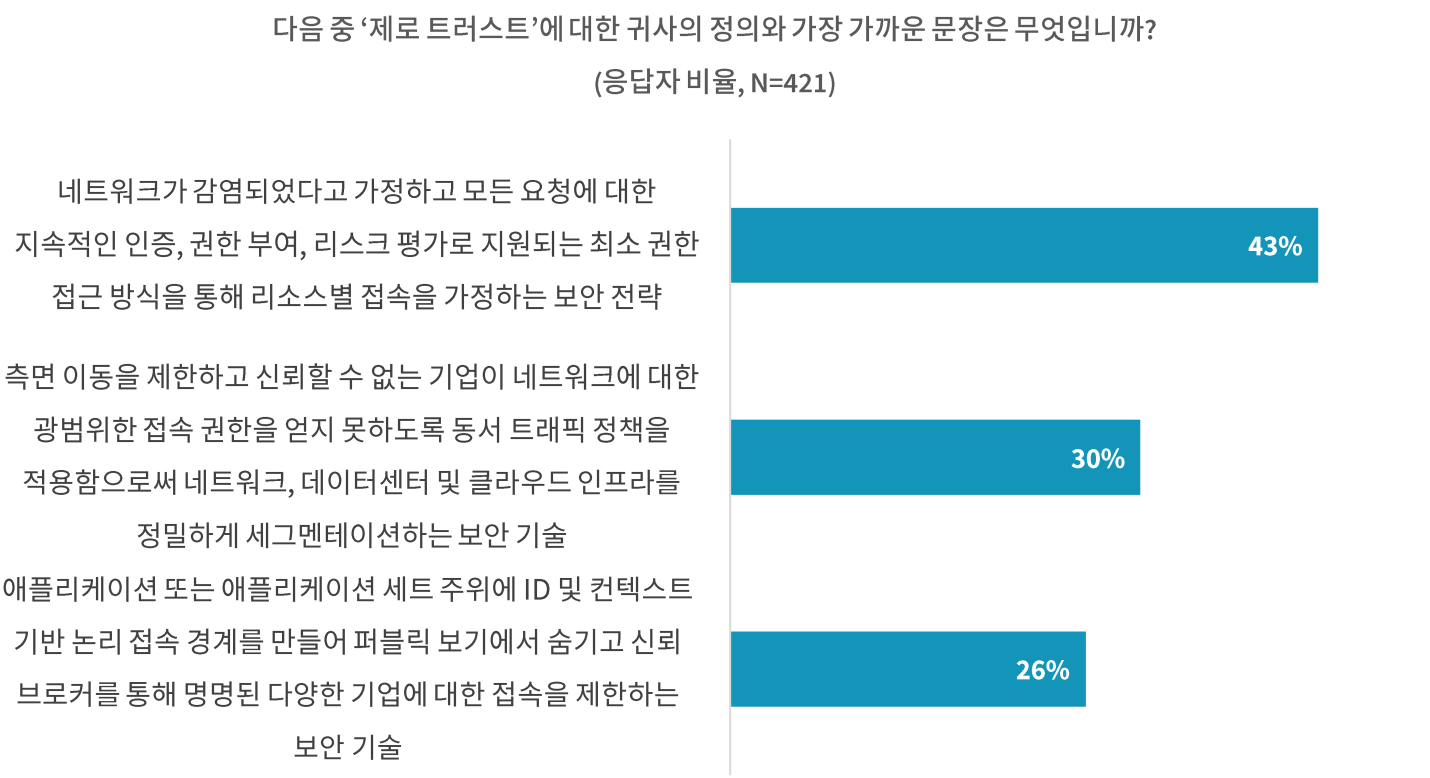
클라우드 컴퓨팅은 그 중요성이 부각되고 보다 전략화됨에 따라, 대부분의 기업에서 사이버 리스크 문제의 중심이 되었습니다. 클라우드 컴퓨팅이 오늘날 IT 전략의 중심이 되면서 제로 트러스트 원칙도 더욱 중요해졌습니다. 기업 및 기업의 클라우드 서비스 파트너는 클라우드 안팎에서 사이버 보안의 역할과 책임에 대한 명확하고 보편적인 이해 기반을 마련하고 이를 동등하게 지원하는 접근 방식을 갖춰야 합니다. 이러한 협업 체계는 기업이 제로 트러스트 모델의 이점을 누릴 수 있는 역량을 최적화하는 데 필수적입니다. 제로 트러스트 모델은 정책 적용의 격차로 발생하는 리스크를 크게 제한하거나, 이상적으로는 완전히 해소할 수 있기 때문입니다.

제로 트러스트의 도입은 최근 몇 년 사이에 크게 증가했으며, 향후 몇 년 동안 거의 모든 환경에 도입될 가능성이 큽니다. 일례로 ESG(Enterprise Strategy Group) 연구 조사에 응답한 응답자 중 46%는 기업 전체에서 제로 트러스트를 구현했거나 구현하기 시작했다고 답했으며, 43%는 특정 사용 사례에 대해 제로 트러스트를 구현했거나 구현하기 시작했다고 답했습니다.

그러나 많은 기업이 제로 트러스트가 무엇이고 제로 트러스트가 무엇을 위해 설계되었는지에 대해 여전히 부정확하거나 심지어 잘못 이해하고 있다는 점은 여전히 중요한 과제로 남아 있습니다.

제로 트러스트를 정의하는 방법은 여러 기업 간에 여전히 근본적인 차이가 있습니다. 예를 들어 ESG 연구에 따르면, 제로 트러스트를 사이버 보안 툴 모음으로 인식하는 기업과 중요한 전략으로 여기는 기업으로 이분화된 것으로 나타났습니다. 제로 트러스트에 대한 기업의 정의를 묻는 질문에 응답자의 43%가 제로 트러스트가 보안 전략이라고 답했으며, 56%는 제로 트러스트가 보안 기술 및 툴과 연관성이 높다고 답했습니다(그림 2 참조). 제로 트러스트와 같은 새로운 트렌드와 관행에 대한 기업의 이분화된 시각이 특이한 일은 아니지만, 오늘날 제로 트러스트를 배포하는 방식에서 비효율성과 혼란을 야기할 수 있습니다.

그림 2: 다양한 제로 트러스트의 정의

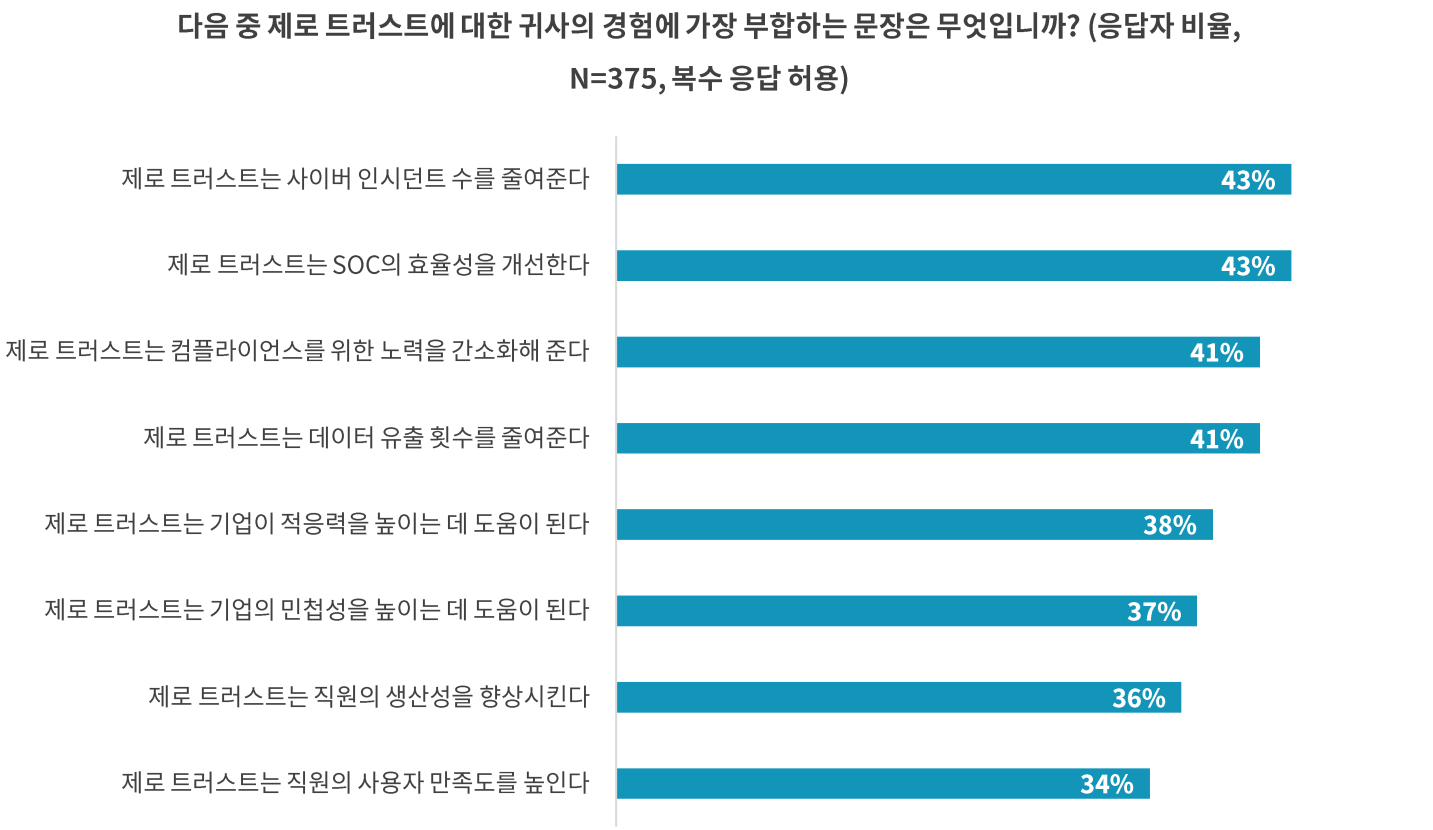


출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

이런 혼란이 여전함에도 불구하고, 제로 트러스트는 가까운 미래에 대한 희망과 좋은 소식을 약속합니다. 제로 트러스트 도입과 같은 기술 트렌드가 약속하는 미래를 확인하는 가장 신뢰할 수 있는 방법 중 하나는 제로 트러스트 모델을 통해 지금까지 달성할 수 있었던 목표에 대한 기업의 신뢰를 확인하는 것입니다.

다행히 많은 기업이 ESG 설문조사에서 제로 트러스트를 처음 구현한 후 성공을 거두고 있다고 말합니다. 더 좋은 소식은 기업이 제로 트러스트 원칙으로 전환하면서 보안과 비즈니스 이점을 모두 경험했다는 점입니다. 예를 들어 거의 절반의 기업이 사이버 인시던트 감소(43%), 사내 보안관제센터(SOC)의 효율성 향상(43%), 컴플라이언스 노력의 간소화(41%), 데이터 유출 감소(41%, 그림 3 참조) 등 다양한 측면에서 제로 트러스트의 이점을 누리고 있다고 답했습니다.

그림 3: 제로 트러스트의 이점



출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

초기에는 특정 사용 사례, 시스템, 부서 및 애플리케이션에 제로 트러스트가 배포되는 경우가 다수였지만, 여기서 얻은 긍정적인 결과가 제로 트러스트의 활용도와 도입률을 높이는 원동력이 될 수 있습니다. 또한 초기 성공 사례가 다양한 부서, 직능 분야 및 지역에서 제로 트러스트 모델에 대한 관심과 도입률을 더욱 높일 수 있습니다.

제로 트러스트의 우선순위 수립

제로 트러스트 전략 수립은 중요하면서도 필수적인 첫 단계이며, 점점 더 많은 기업이 제로 트러스트 전략을 수립하는 상황은 긍정적인 발전임이 분명합니다. 그러나 실제로 제로 트러스트에 관한 종합적인 이니셔티브를 구현하기란 쉽지 않으며, 기업은 구현 단계의 우선순위를 정하는 방법을 철저하게 분석하고 평가해야 합니다.

이때 다양한 사이버 보안 부문이 관여하며, 제로 트러스트 전략을 지원할 수 있는 많은 기술이 존재합니다. 가장 짧은 시간 안에 가장 큰 영향력을 발휘할 수 있도록 초기에 배포할 툴과 집중해야 할 영역을 적절히 계획하고 우선순위를 정하는 것이 매우 중요합니다.

제로 트러스트로 가는 경로는 다양하지만, 제로 트러스트와 보다 깊이 관련되어 있으면서도 다른 것들보다 우수한 몇 가지 툴, 기술, 기법이 있습니다.

예를 들면 다음과 같습니다.

- **세그멘테이션 및 마이크로세그멘테이션** 제로 트러스트의 핵심은 정책에서 지정한 경우에만 기업이 서로 통신할 수 있다는 데 있습니다. 대략적인 수준의 세그멘테이션으로도 사용자 및 디바이스에서 접속할 수 있는 환경의 구성 요소들을 제한할 수 있습니다. 예를 들어, 기업은 연결된 의료 디바이스가 금융 애플리케이션이 상주하는 위치와 동일한 네트워크에 접속할 수 없도록 제한할 수 있습니다. 그러나 이 방법으로는 진정한 제로 트러스트 접근 방식에 필요한 수준의 정밀도를 얻을 수 없습니다. 그래서 마이크로세그멘테이션을 통해 워크로드 수준에서 정책을 보다 구체적으로 생성하고 공격자의 측면 이동을 방지하는 방법에 대한 관심이 높아지고 있습니다.

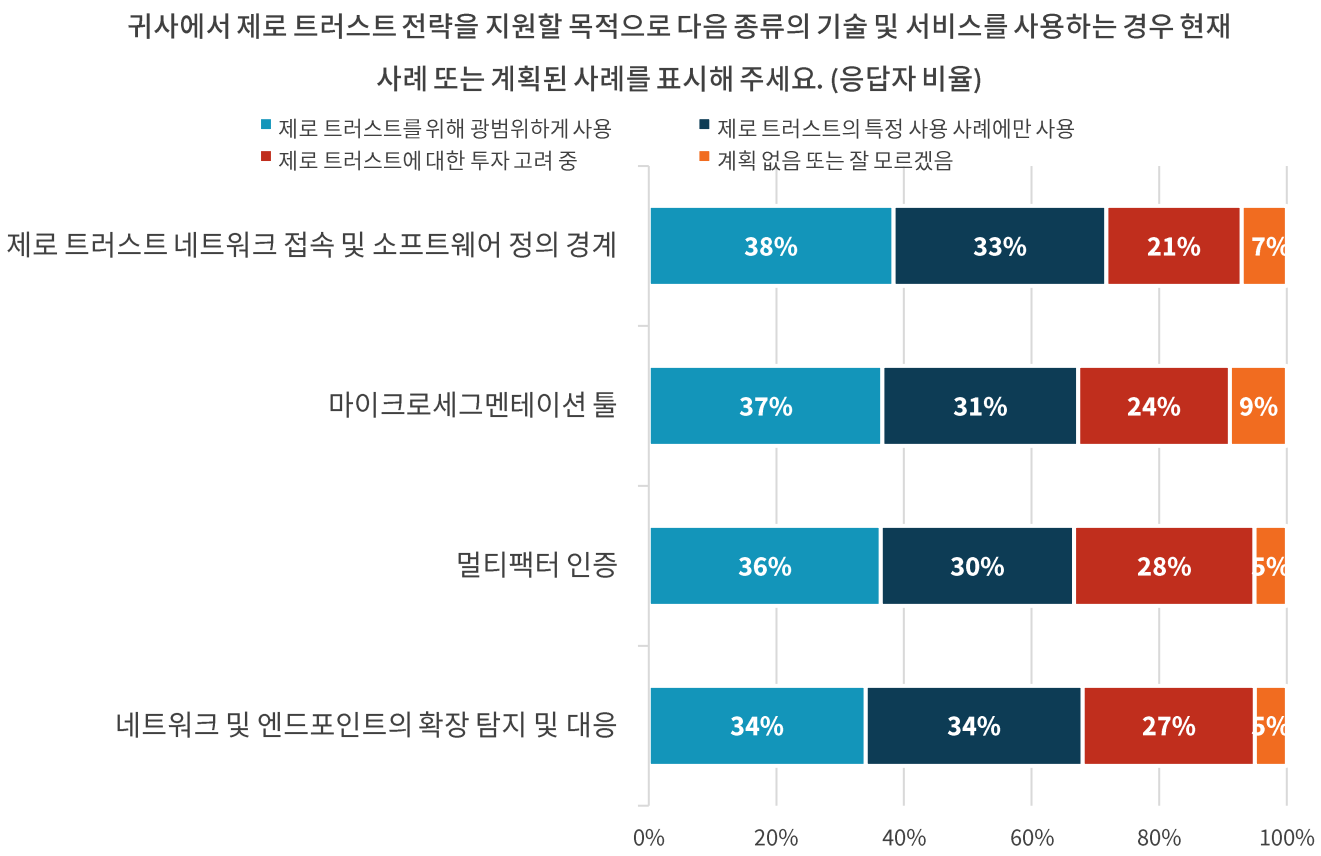
- **멀티팩터 인증과 비밀번호 및 비밀번호 없는 ID 프레임워크를 포함한 ID 전략** 기업의 사이버 보안에서 ID 도용이 더 확대되고 교묘해지는 만큼, 제로 트러스트 원칙을 통해 기업 내부와 외부 모두에서 ID 도용을 근본적으로 차단하는 것이 보안을 보다 효과적으로 유지할 수 있는 현명한 방법입니다.

- **제로 트러스트 네트워크 접속(ZTNA).** VPN과 같이 애플리케이션에 대한 원격 접속을 가능케 하는 기존의 접근 방식은 실제로 사용자에게 네트워크 수준의 접속 권한을 제공합니다. 공격자가 무단 접속 권한을 얻으면 네트워크를 통해 측면으로 이동할 수 있습니다. 반면, ZTNA는 ID를 기반으로 애플리케이션 접속을 지원하므로 측면 이동의 가능성을 줄여줍니다.

- **탐지 및 대응.** 기업은 '신뢰할 수 있는' 정책을 위반하는 작업이 있을 경우 이를 신속하게 파악하고 대응해야 합니다. 사이버 보안 기업의 경우 '경보 피로'가 점점 더 큰 문제로 부각되고 있으며, 이상 행동과 잠재적 위협을 선별하는 보다 정밀하면서도 컨텍스터에 기반한 접근 방식이 필요합니다. 신뢰 기반 정책을 수립하면 탐지 및 대응의 효율성과 효과를 높일 수 있습니다.

ESG(Enterprise Strategy Group) 연구는 제로 트러스트 프레임워크를 실제로 구현하려는 경우 앞서 언급한 우선순위와 기타 우선순위가 중요하다는 점을 강조합니다. 예를 들어 대부분의 기업에서는 제로 트러스트 모델의 일부로 ZTNA를 광범위하게 혹은 특정 사용 사례(71%)에 활용합니다. 기업에서 제로 트러스트 모델의 일부로 사용되는 기타 기술 및 서비스로는 네트워크 및 엔드포인트 EDR(68%), 마이크로세그멘테이션 툴(68%), 멀티팩터 인증(66%, 그림 4 참조)이 있습니다.

그림 4: 제로 트러스트를 지원하는 데 사용되는 기술



출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

제로 트러스트를 향한 Akamai의 접근 방식

Akamai는 많은 사례를 통해 기업이 최종 사용자 측에 애플리케이션을 효과적으로 전송하고 보호하도록 지원하는 역량을 입증했습니다. Akamai는 수년간 기업 보안 기능을 꾸준히 추가해 왔으며, 이제 기업이 사람, 사물, ID를 아우르는 제로 트러스트 보안 체계를 구축할 수 있도록 지원할 수 있는 다양한 제품을 선보이고 있습니다.

Akamai는 Guardicore를 인수하면서 정책에서 명시적으로 허용하지 않는 한 워크로드와 애플리케이션 간 통신을 기본적으로 거부하는 호스트 기반 마이크로세그멘테이션 솔루션을 제공합니다. 이 솔루션을 통해 고객은 공격표면을 줄이고, 측면 이동을 차단하며, 랜섬웨어로부터 중요한 자산을 보호하고, 모든 환경(온프레미스, 클라우드, IoT 및 OT)에 제로 트러스트 정책을 자동으로 적용할 수 있습니다.

Akamai Hunt는 측면 이동, 멀웨어 실행, 명령 및 제어 서버와의 통신, 사용자 및 네트워크 이상 징후 등과 같은 공격 행위를 검색하고 고객에게 경고하는 매니지드 위협 탐지 서비스입니다. 고객은 전문 연구원으로 구성된 팀의 도움으로 방어 권장 사항을 비롯해 보안 리스크에서 우선순위가 높은 알림만 받을 수 있습니다.

Akamai의 Enterprise Application Access는 강력한 인증과 컨텍스트를 기반으로 프라이빗 애플리케이션에 대한 정밀한 최소 권한 접속 정책을 적용하는 클라우드 기반의 제로 트러스트 네트워크 접속 솔루션입니다.

Akamai MFA는 강력한 사용자 인증을 제공하는 FIDO2 기반의 피싱 방지 MFA 서비스입니다. 직원 계정 탈취를 차단하는 데도 효과적입니다. 이 솔루션은 기업이 추가 ID 확인 메커니즘을 보안 정책에 계층화하고 비밀번호 없는 인증으로 전환하도록 지원하는 원활한 인증 솔루션입니다.

마지막으로 Akamai의 Secure Internet Access는 인터넷 기반 리소스에 접속하는 사용자와 디바이스를 멀웨어, 랜섬웨어 및 기타 위협으로부터 보호하는 보안 웹 게이트웨이입니다. 또한 허용 가능한 사용 정책을 준수하고 민감한 데이터가 실수로 또는 악의적으로 외부 사이트 및 애플리케이션에 업로드되지 않도록 하는 데 도움을 줄 수 있습니다.

이러한 광범위한 기능 덕분에 Akamai는 제로 트러스트 여정을 막 시작했거나 이미 시작한 모든 기업의 매력적인 파트너가 될 수 있습니다.

결론

사이버 보안은 기업, 산업 및 사회가 디지털화됨에 따라 점점 더 어려워지고 복잡해질 것입니다. 그 결과, 유출, 침입, 데이터 손실 및 디지털 자산 감염으로 인한 영향은 더욱 커지고, 광범위해지며, 더 큰 문제로 이어질 수 있습니다.

제로 트러스트는 모든 기업의 사이버 보안 전략의 핵심이 되어야 하며 마이크로서비스 및 기타 지원 기술은 제로 트러스트를 배포하는 방법, 시기 및 위치에 대한 정보를 제공하고 구체화하며 영향을 줄 수 있어야 합니다.

제로 트러스트 및 마이크로서비스에 대한 Akamai의 접근 방식은 사이버 보안 전략에 대한 포괄적이면서도 미래 지향적이고 혁신적인 시각을 제시하므로, 기업은 이를 통해 클라우드 중심으로 변화하는 환경에서 디지털 자산을 효과적으로 방어할 수 있습니다.

Enterprise Strategy Group은 글로벌 기술 커뮤니티에 마켓 인텔리전스, 실행 가능한 통찰력 및 GTM(Go to Market) 콘텐츠 서비스를 제공하는 통합 기술 분석, 연구 및 전략 회사입니다.

www.esg-global.com

contact@esg-global.com

508.482.0188