ivanti

Cybersecurity
INSIDERS

2021년 제로 트러스트 진행 보고서

ivanti.com

개요

기업의 제로 트러스트 보안 모델 채택은 대부분의 조직이 특히나 원격 근무로의 대대적인 전환으로 인해 증가하고 있는 사이버 위협을 완화하기 위해 그 어느 것도 신뢰하지 않는 제로 트러스트의 역량을 구현하면서 가속화되고 있습니다. 최소의 권한을 기반으로 한 조건적인 접근을 허용하기 전에 사용자와 기기를 검증한다는 원칙으로, 제로 트러스트는 현저하게 강화된 사용성, 데이터 보호 및 거버넌스를 보장합니다.

2021년 제로 트러스트 보고서는 핵심적인 추진 요소들, 채택 동향, 기술력, 투자 및 혜택을 포함하여 기업들이 조직 내에서 어떻게 제로 트러스트 보안을 구현하고 있는지를 보여줍니다.

이 정보를 제공하기 위해 여러 산업계에서 다양한 규모의 조직들을 균형 있게 대표하는 기술 임원부터 IT 보안업계 종사자들까지 사이버 보안 전문가들을 상대로 설문조사를 수행했습니다.

핵심적인 발견 사항은 다음과 같습니다.

- 사용자, 기기 및 인프라 요소를 포함하여 주체 검증을 통해 확보한 신뢰(64%)는 제로 트러스트의 핵심적인 요소의 상위 차지합니다. 다음으로는 데이터 보호(63%)와 지속적인 인증/승인(61%)이 따릅니다.

- 사용자들이 적절한 수준의 접근 권한을 가지도록 제한하기 위해 모든 사용자에게 현재의 접근 권한 결정하는 것은 어려운 작업입니다. 조직의 3/4 이상(88%)은 사용자들이 필요 이상의 접근 권한을 가지고 있음을 알 수 있습니다.

- 현재의 보안 우선순위에 대해 물어봤을 때,사이버 보안 전문가들은 가장 먼저 개선된 계정 접근 관리(68%)을 언급했고, 그 다음으로 데이터 유출 방지(56%), 그리고 보안 애플리케이션 액세스(46%)에 대해 언급했습니다.

이 중요한 연구 프로젝트를 지원한 Ivanti 에 많은 감사 드립니다.

이 보고서가 귀사의 IT 환경을 보호하는 데 유용하며 도움이 되는 정보이길 희망하는 바입니다.

감사합니다.

Holger Schulze

Holger Schulze
CEO 겸 설립자
Cybersecurity Insiders

Cybersecurity
INSIDERS

제로 트러스트 원리

저희는 조직에 제로트러스트의 어떤 측면이 가장 매력적이라고 생각하는지 물었습니다. 사용자, 기기 및 인프라 요소를 포함하여 주체검증을 통해 확보한 신뢰(64%)는 제로 트러스트의 핵심적인 요소의 상위를 차지합니다. 다음으로는 데이터 보호(63%) 와 지속적인 인증/승인(61%)이 따릅니다.

귀하와 귀사는 제로 트러스트 원칙의 어떤 면이 가장 매력적이라고 생각하십니까?[1]

64%

주체 검증을 통해 확보한 신뢰(예: 사용자, 기기, 인프라)

63%

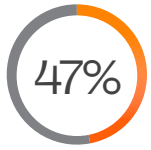
데이터 보호(예: 보호된 연결)

61%

지속적인 인증/승인

종단 간 접근 가시성 및 감사

최소한의 접근 권한 부여



중앙화의 더욱 세밀화된 접근 정책

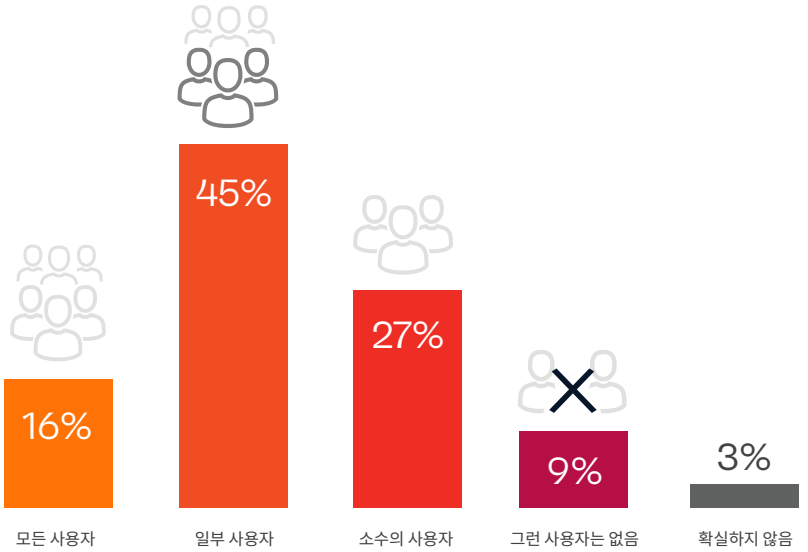
내부 또는 외부 네트워크 간에 신뢰가 없는 점

과도한 접근 권한

사용자들이 적절한 수준의 접근 권한을 가지도록 제한하기 위해 모든 사용자들에게 현재의 접근 권한을 결정하는 것은 어려운 작업입니다. 조직의 3/4 이상(88%)은 사용자들이 필요 이상의 접근 권한을 가지고 있음을 알 수 있습니다.

조직 내 어느 정도의 사용자들이 필요 이상의 접근 권한을 가지고 있는 상황이라고 생각하십니까?

88% 는 사용자들이 필요 이상의 접근 권한을 가지고 있다고 알려져 있습니다.



보안 우선순위

현재의 보안 우선순위에 대해 물어봤을 때, 사이버 보안 전문가들은 가장 먼저 개선된 계정 접근 관리(68%)을 언급했고, 그 다음으로 데이터 유출 방지(56%), 그리고 보안 애플리케이션 액세스(46%)에 대해 언급했습니다.

현재 귀사의 보안 우선순위는 무엇입니까?[2]

68%

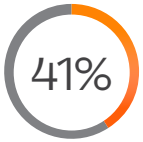
개선된 계정 접근 관리 (Improve Identity and Access Management, IAM)

56%

데이터 유출 방지 (Data Loss Prevention, DLP)

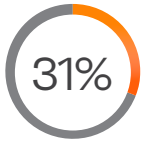
46%

클라우드 서비스 제공업체가 호스팅하는 애플리케이션에 대한 안전한 접근 보장(예 Microsoft, Amazon, Google)



엔드포인트 모바일 관리(Enable Endpoint Mobile Management, EMM)/BYOD (예: 사용자 기기)

엄격한 SSL 점검 수행(예: 멀웨어 스캐닝 및 웹/이메일 필터링을 위해 안전한 세션 암호화)



안전한 접근 제공의 단순화(예: 사용자 체험, 관리)

기존 원격 접근 도구 강화 혹은 교체(예: VDI, VPN, RDP)

계정 접근 관리 및 제로 트러스트 우선순위

조직들이 어떤 계정 접근 관리 및 제로 트러스트 통제에 투자하고 있는지를 물어봤습니다. 우선순위는 투자 관점에서 다단계 인증(58%), 다음으로 계정 관리 및 거버넌스(48%), 그리고 싱글 사인온(45%)이었습니다.

다음 12개월 내로 계정 접근/제로 트러스트 통제의 어떤 점을 조직의 투자를 위해 우선 순위를 정하시겠습니까?[3]

58%

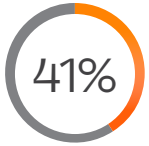
다단계 인증 (Multi-Factor Authentication, MFA)

48%

계정 관리 및 거버넌스

45%

싱글 사인온 (Single Sign-On, SSO)



특권 접근 관리 (Privileged Access Management, PAM), 마이크로 세분화 (Micro-segmentation)

가상 사설망 (Virtual Private Network, VPN)

마이크로 세분화 (Micro-segmentation)

네트워크 접근 제어 (Network Access Control, NAC), 웹 애플리케이션 방화벽 (Web Application Firewall, WAF)

안전한 접근 우선순위

안전한 접근 우선순위에 대해 구체적으로 물어봤을 때, 조직들은 다단계 인증/특권 접근 관리(69%)를 우선 순위로 정하였습니다. 다음으로는 익명 활동 탐지와 대응(58%), 그리고 개인용 및 관리되지 않는 기기로부터의 안전한 접근(55%)이었습니다.

다음 1년~2년간 귀하의 안전한 접근에 대한 우선순위는 무엇입니까?

69%

다단계 인증/ 특권 접근 관리

58%

익명 활동 탐지와 대응

55%

개인용 및 관리되지 않는 기기로부터의 안전한 접근

레거시 보안 인프라 재평가 및 소프트웨어 정의 접근 고려

경영진에 대한 더욱 강력한 가시성 및 보안 매트릭스

마이크로 세분화 (Micro-segmentation)

안전한 접근 도전 사항

앱과 자원으로 안전한 접근에 대해 가장 우려되는 사항은 특권 접근(60%), 그 다음으로 파트너들에게 안전한 접근 제공(50%)으로 이들은 제로 트러스트를 통해 직접 해결됩니다.

앱이나 자원으로의 안전한 접근 면에서 현재 귀사가 경험하는 어려움은 무엇입니까?

60%

지나치게 권한이 주어진 직원 접근

50%

파트너가 앱이나 자원에 안전하지 않은 방법으로 접근

47%

사이버 공격(예: 서비스 거부, 크로스 사이트 스크립팅, 중간자, 피싱 공격)

쉐도우 IT

수동 프로세스는 복잡하여 신속한 대응력을 저해함

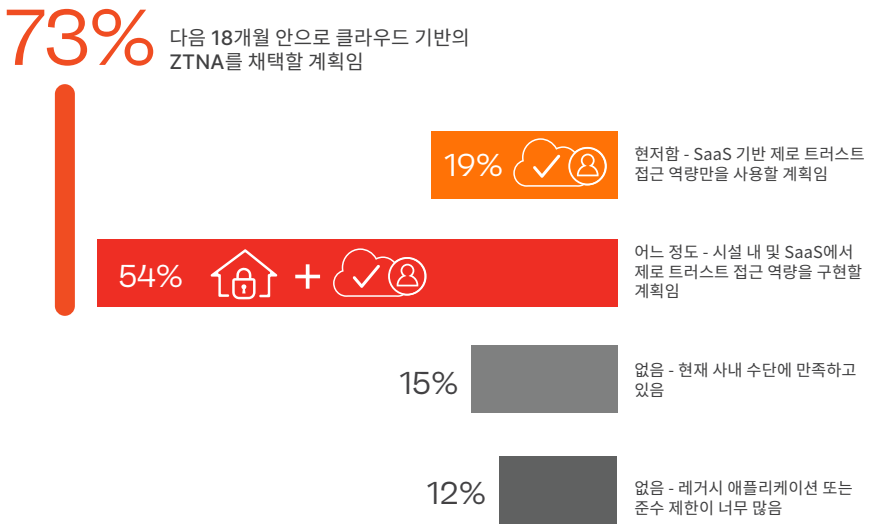
취약하거나, 탈옥하거나, 또는 잃어버린 모바일 장치가 자원에 접근

위험한 디바이스(알려지지 않은, 비인가된, 비준수 엔드포인트)를 통한 네트워크 자원 접근

제로 트러스트 SaaS

보안은 클라우드로 옮겨가고 있으며 ZTNA도 예외가 아닙니다. 응답자들 중 거의 3/4가 다음 18개월 안으로 클라우드 기반의 ZTNA 솔루션을 채택할 계획입니다.

다음 18개월 안으로 귀하나 귀사가 제로 트러스트 접근 역량을 SaaS로 옮길 가능성은 얼마나 된다고 생각하십니까?



개인용 앱 접근

개인적인 앱을 보호하는 데 조직들이 경험하는 가장 어려운 점에 대해 물어봤습니다. 반 이상의 응답자들은 공공 클라우드 환경에서 배포되는 애플리케이션에 안전하게 접근하는 것이 오늘날의 가장 큰 어려움이라고 합니다(54%).

개인용 앱으로의 접근을 보호하는 데 있어 다음의 요소들을 어려운 점에 기반하여 순위를 매겨주십시오?

54% 공공 클라우드에 있는 앱에 접근

29% 데이터 센터에 있는 앱에 접근

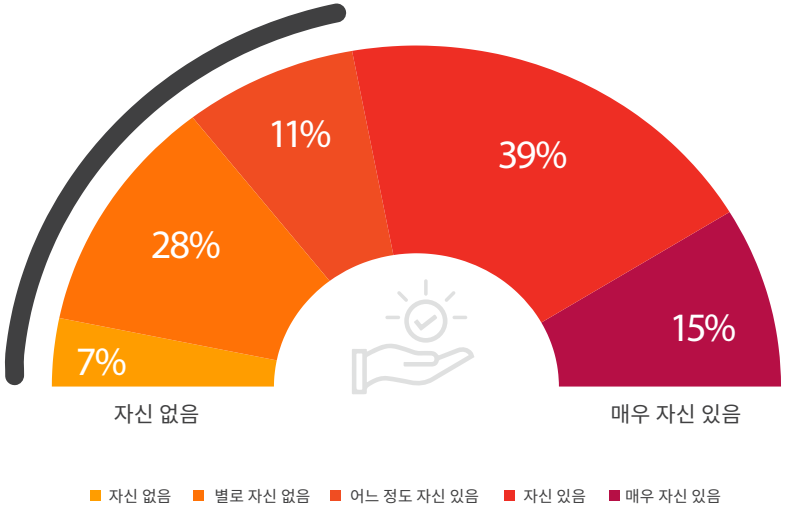
17% 본사에 있는 앱에 접근

제로 트러스트 자신감

제로 트러스트 적용 능력에 대한 자신감에 대해 물었을 때 거의 반 정도의 기업 IT 보안 팀은 자신이 없음을 나타냈습니다(46%).

안전한 접근 아키텍처에 제로 트러스트 모델/원리를 적용하는 데 얼마나 자신감이 있으십니까?

46% 의 기업 IT 보안 팀은 제로 트러스트를 제공하는 자체 능력에 자신 없음을 나타냈습니다.



공공 클라우드에 있는 앱에 접근

전통적인 원격 접근 솔루션은 오늘날의 역동적이며 분산된 클라우드 환경에서 실패하고 있습니다. 안전한 접근을 제공할 때 사이버 보안 전문가들이 경험하게 되는 상황에 대해 물어봤을 때 가장 많이 언급된 사항은 공공 앱 클라우드에 접근하기 위해 데이터 센터를 통해 원격 또는 모바일 사용자들을 “헤어피닝(hairpinning)”하는 것이라고 합니다. 37%라는 놀라운 수가 원격 및 모바일 사용자들을 활성화하기 위해 클라우드 앱을 공개적으로 노출해야만 하며 이는 현저한 위험에 노출하게 되는 상황입니다.

원격 또는 모바일 사용자들을 위해 공공 클라우드 앱으로의 안전한 접근을 제공할 때 다음 중 어떤 상황을 경험해 보셨습니까?

47%

공공 클라우드에 있는 앱을 접근하기 위해 자사 데이터 센터를 통해 원격사용자를 ‘헤어핀’ 해야함

37%

접근을 제공하기 위해 공공 클라우드에 개인용 앱을 공개적으로 노출해야 함

35%

공공 클라우드 환경에서 자사에서 선호하는 원격 VPN 장비를 배포할 수 없음

제로 트러스트 추진 요소

조직들로 하여금 제로 트러스트를 시작하거나 확장하게 하는 요인은 무엇입니까? 데이터 보안(82%) 상위를 차지했으며, 그 다음으로 침해 방지(68%), 엔드포인트에 대한 위협 감소(53%)가 따랐습니다.

귀사로 하여금 계정 접근/제로 트러스트를 시작하거나 확장하게 하는 주요 요인은 무엇입니까?[4]

82%
보안/데이터 보호

68%
침해 방지

53%
엔드포인트 및 IoT 보안 위협 감소

내부자 위협 감소

업계/규제 당국 준수 (예: HIPAA, GDRP, PCI DSS)

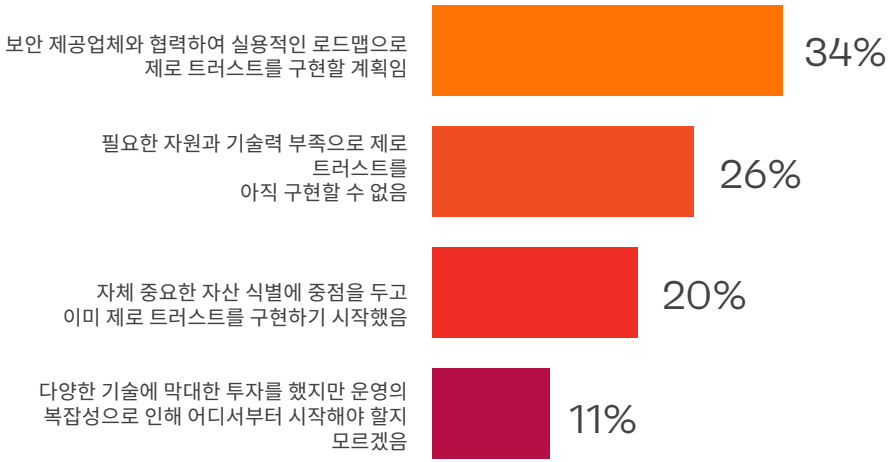
하이브리드 IT 보안 문제 해결

운영적 효율성

제로 트러스트 구현

제로 트러스트는 신속하게 가속화되고 있으며 조직들은 이 기술을 구현하는 데 여러 가지 다른 경로를 채택합니다. 조직들이 채택하는 가장 일반적인 접근법은 보안 제공업체와의 협업으로 실용적인 로드맵을 구축하여 제로 트러스트를 구현하는 것입니다(34%). 하지만 필요한 자원과 기술력 부족(26%)은 제로 트러스트에 대해 중요한 장애물로 남아 있습니다.

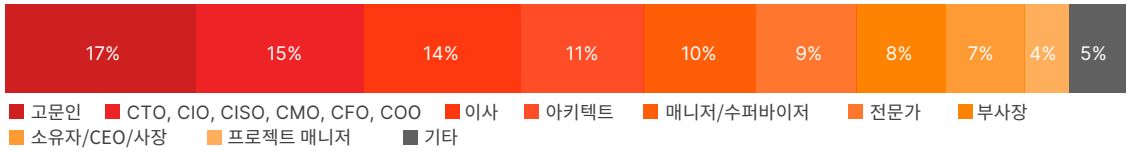
제로 트러스트 구현이 점진적인 프로세스라면, 확장된 환경까지 전반에 걸쳐 제로 트러스트를 어떻게 구현하실 계획입니까?[5]



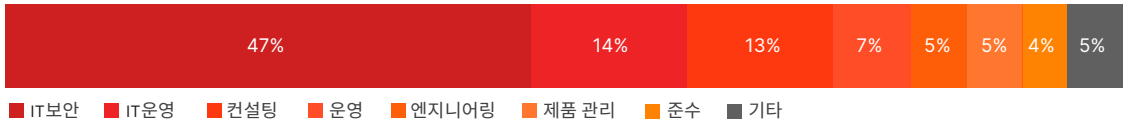
방법론 및 통계정보

이 보고서는 미국 내 443명의 IT 및 사이버 보안 전문가들을 상대로 2021년 7월 수행된 광범위한 온라인 설문조사를 기반으로 한 것이며, 이 설문조사의 목표는 제로 트러스트와 관련된 최신 기업 채택 동향, 도전 사항, 격차, 솔루션 선호도를 파악하는 것이었습니다. 응답자들은 여러 산업계에서 다양한 규모의 조직들의 균형 있게 대표하는 기술 임원부터 IT 보안업계 실무자까지 다양합니다.

경력 수준

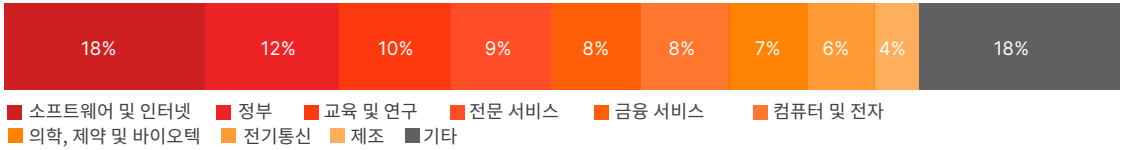


부서



업체 규모

업계



ivanti.com
+81 6432 4180
sales@ivanti.com

Ivanti는 Everywhere Workplace(어느 곳이나 근무지)를 가능하게 합니다. Everywhere Workplace에서 직원들은 다양한 네트워크상에서 다양한 기기를 이용하여IT 애플리케이션과 데이터에 접근하고 어디서나 근무함으로써 생산성을 유지합니다.

Ivanti Neurons 자동화 플랫폼은 회사의 업계를 선도하는 일관된 엔드포인트 관리인 제로 트러스트와 기업 서비스 관리 솔루션을 연결하여 통합된 IT 플랫폼을 제공하고 기기들이 스스로 수리하고 보호할 수 있도록 하며 사용자들은 셀프 서비스로 더 큰 역량을 보유할 수 있습니다.

포천지 선정 100대 기업 중 78개 업체를 포함하여 40,000명이 넘는 고객들은 클라우드로부터 에지까지 Ivanti를 선택하여 그들의 IT 자산을 발견하고, 관리하며, 보호하고, 제공하여 직원들이 어디에서 어떤 방식으로 근무하더라도 최고의 최종 사용자 체험을 제공할 수 있도록 합니다.

좀 더 자세한 정보는 www.ivanti.com 을 방문하고 @GoIvanti 를 팔로우하세요.

1 자원 통합 40% | 기타 2%

2 추가 엔드포인트 탐지 및 대응(Endpoint Detection and Response, EDR) 28% | 강화 SD-WAN 보안 기능 27% | 향상된 취약성 완화(예: 취약성 관리, 패치 관리) 5% | 더 나은 모바일 위협 보호 제공(모바일 위협 방어/안티피싱)2% | 없음 2% | 기타 4%

3 웹 애플리케이션 방화벽(Web Application Firewall, WAF) 35% | 엔터프라이즈 모바일 관리(Enterprise Mobile Management, MDM) 31% | 클라우드 보안 접속 브로커(Cloud Access Security Broker, CASB) 30% | 아이덴티티 애널리틱스 27% | 소프트웨어 정의 경계(Software Defined Perimeter, SDP) 26% | 엔터프라이즈 디렉터리 서비스 17% | 제로 트러스트 네트워크 접근에 대한 완전한 통제 12% | 취약성 관리/ 패치 관리 9% | 위협에 대한 네트워크 기기 비가시성 7% | 안티피싱 7% | 모바일 위협 방어 5% | 기타 2%

4 사내 준수 28% | 감사 또는 보안 사건에 대한 대응 28% | 기타 5%

5 기타 9%