Gigamon®

설문조사 보고서

2023 하이브리드 클라우드 보안 설문조사

인식 vs. 현실

목차

서론

비용 증가와 경제적 불확실성이 클라우드 마이그레이션의 속도 둔화를 야기하고 있는 가운데 여전히 대다수 조직은 하이브리드 인프라를 유지하고 있습니다. Forrester의 애널리스트들은[1] 이를 매우 일반적인 현상으로 간주합니다. 보고서에 따르면 전체 조직의 **72%**가 하이브리드 클라우드에서 운영되고 있습니다.[2] 그 배경에는 기업이 인수 또는 다양한 이점을 얻기 위한 노력의 일환으로 자체 데이터 센터/프라이빗 클라우드를 하나 이상의 퍼블릭 클라우드와 결합할 가능성이 높다는 이유가 있습니다. 예를 들어, Cisco는 **42%**의 조직이 하이브리드 클라우드를 통해 보다 민첩하고 확장 가능한 개발 환경을 구현했다고 답했으며 비즈니스 민첩성 및 혁신을 가속화했다고 답한 비율은 **40%**에 이른다고 밝혔습니다.[3]

하지만 클라우드 기반 보안 위협 및 침해의 급격한 증가에 따라 하이브리드 클라우드 보안이 CISO, CIO 및 관련팀의 최우선 순위로 부상하면서 고려해야 할 사항도 더욱 다양해졌습니다.

Gigamon의 이번 최신 보고서는 하이브리드 클라우드 보안과 관련해 우리 눈에 보이는 모든 것이 현실과는 다를 수도 있음을 강조합니다. 실제 연구 결과, 이러한 인프라 보안에 대한 우리의 인식과 현실 간에 격차가 존재한다는 것이 밝혀졌습니다. 초기 질문에서 CISO, 클라우드 아키텍트, 클라우드 보안 분석가를 포함한 전 세계 IT 및 보안 리더들은 자사의 보안 도구 및 프로세스가 하이브리드 클라우드 인프라에 대해 제공하는 가시성과 인사이트가 완벽하다는 자신감을 드러냈습니다. 이러한 비율은 소수가 아닌 **94%**의 높은 수치를 보였습니다. 하지만 정확한 딥 옵저버빌리티 수준을 파악하기 위한 심층적인 조사에 들어가자 암호화된 트래픽, 측면 이동 데이터 및 '알려지지 않은' 사각지대에서 중대한 가시성 격차가 나타나기 시작했습니다.

예를 들어, 설문조사에 참여한 글로벌 IT 및 보안 리더의 **절반**이 온프레미스에서 클라우드에 이르는 하이브리드 클라우드 인프라 전반에서 충분한 보안을 구현하고 있다는 자신감 또는 완벽한 자신감이 있다고 답한 반면 **90%**는 지난 18개월 동안 데이터 침해로 인한 어려움이 있었음을 인정했습니다. 이를 바탕으로 Gigamon은 하이브리드 클라우드 인프라 보안에 대한 조직의 인식과 실제 데이터 보호 수준 간에 상당한 차이가 존재한다는 것을 알 수 있었습니다.

실제 현실에서는 본 '하이브리드 클라우드 보안: 인식 vs. 현실' 보고서의 설문조사에 참여한 거의 모든 응답자가 데이터 침해를 경험했습니다. 여기에서 가장 우려되는 점은 IT 및 보안 전문가들이 이러한 침해를 탐지하지 못한 경우가 많았다는 것입니다. 또한 영국, 프랑스, 독일, 미국, 호주, 싱가포르 등 6개 주요 글로벌 시장에서 수집한 자료는 기술 격차, 불충분한 사이버 투자 등 보안 리더들이 갖고 있는 대표적인 두려움들이 실제로는 핵심적인 문제가 아니라는 사실을 강조했습니다. 전송 중인 모든 데이터 전반에 걸친 실시간 인사이트, 즉 딥 옵저버빌리티를 확보하는 것이 그 어느 때보다 중요해진 오늘날의 현실이 그 근거가 되고 있습니다.

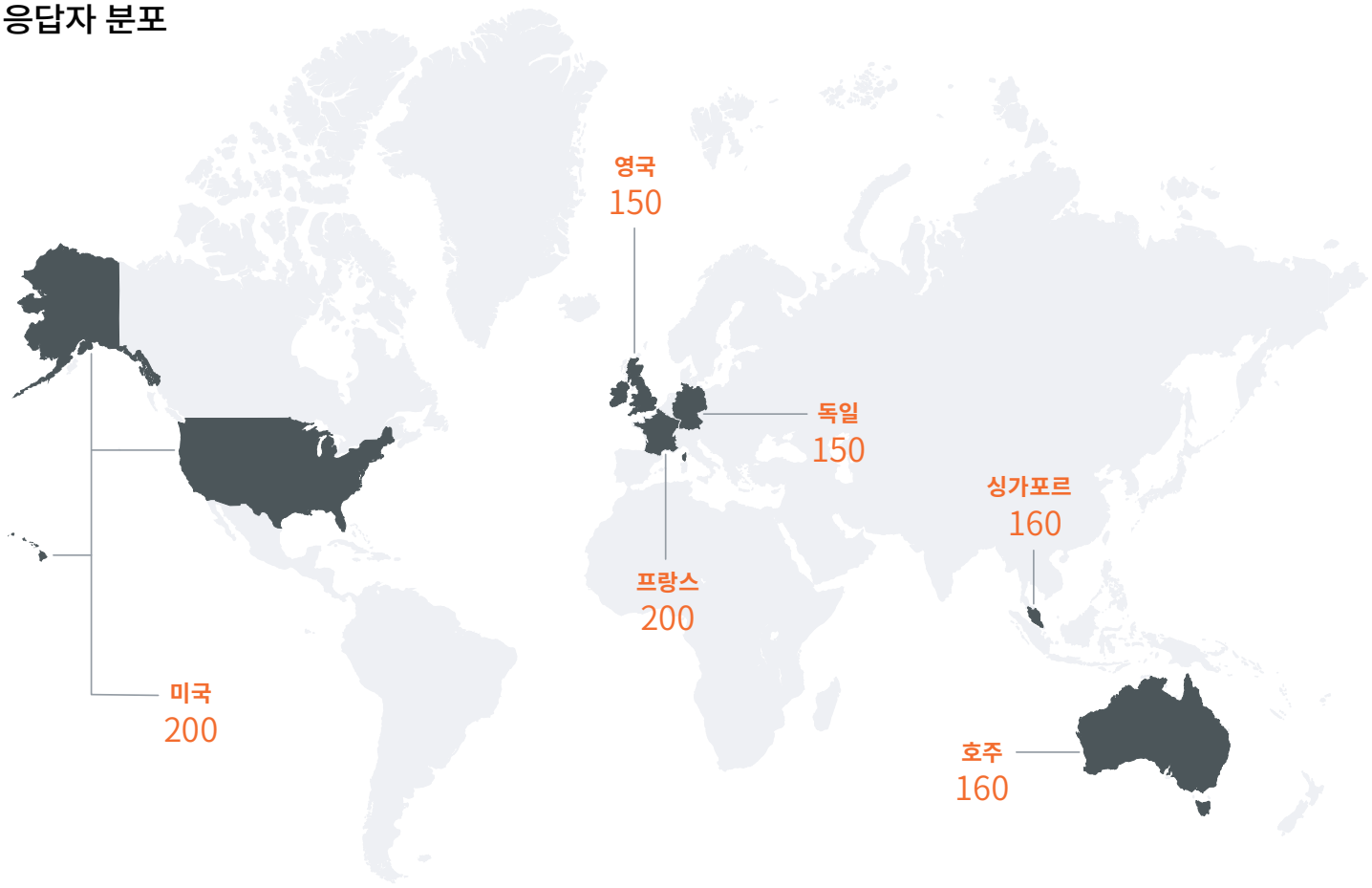
Gigamon은 '딥 옵저버빌리티'를 실행 가능한 네트워크 유래 인텔리전스 및 인사이트를 이용한 기존 보안 및 옵저버빌리티 도구의 성능 증폭으로 정의합니다. 이는 보안 및 성능 사각지대를 제거할 뿐만 아니라 팀이 하이브리드 클라우드 보안 및 규정 준수 위험을 선제적으로 완화하고 우수한 디지털 경험을 제공하며 급증하는 하이브리드/멀티 클라우드 인프라 관리 비용 및 복잡성을 억제할 수 있도록 합니다. 클라우드 기반 공격의 증가가 예상되는 오늘날 이러한 향상된 가시성을 확보하는 것은 필수입니다.

방법

본 보고서에 사용된 데이터는 Vitreous World가 온라인 방식을 이용해 모집한 다양한 CIO, CISO, CTO, COO, 클라우드 보안 분석가, 클라우드 엔지니어, 클라우드 아키텍트, 정보 보안 VP 및 기타 네트워킹 담당자에게서 수집했습니다. 인터뷰는 영국, 프랑스, 독일, 미국, 호주, 싱가포르에서 수행되었습니다. 또한 본 연구에 참여한 모든 응답자는 익명성 유지를 보장받았습니다. 현장 조사는 2023년 4월 19일부터 5월 2일까지 수행되었습니다. 표본은 다음과 같은 전문가로 구성되었습니다.

- **총 1,020명의 응답자:** 영국(150명), 프랑스(200명), 독일(150명), 미국(200명), 호주(160명), 싱가포르(160명)
- **42%**는 직원 수 501~1,000명의 기업, **58%**는 직원 수 1,000명 이상 기업에 근무합니다.
- 직위: 최고정보책임자(**15%**), 최고 기술 책임자(**5%**), 최고 정보 보안 책임자(**12%**), 클라우드 엔지니어(**7%**), 클라우드 보안 분석가(**4%**), 정보 보안 VP(**5%**)

응답자 분포



주요 내용

1. 하이브리드 클라우드 보안에 대한 인식과 현실에 차이가 있습니다.

설문조사에 참여한 IT 및 보안 리더의 **50%**가 온프레미스에서 클라우드에 이르는 IT 인프라 전반에서 충분한 보안을 구현하고 있다는 자신감 또는 완벽한 자신감이 있다고 답했습니다. 하지만 이와 동시에 대다수가 지난 18개월 동안 데이터 침해로 인한 어려움이 있었다고 답했는데 이는 보안에서는 만족감을 가지는 것이 위험하다는 것을 강조합니다.

2. IT 및 보안 전문가들은 보안 침해의 약 1/3을 탐지하지 못하고 있습니다.

표면적으로 전체 하이브리드 클라우드 가시성 및 보안에 대한 자신감이 높게 나타나고 있지만 실제로 전체 침해의 약 1/3은 (DoS 또는 전송 중 유출 등으로 인해) 다크웹에 데이터가 나타나거나 파일 액세스가 불가능해지거나 사용자가 애플리케이션 성능 지연을 경험하는 등의 사건이 발생한 후에야 식별됩니다. 이를 통해 위협 탐지 및 식별을 위해서는 기존 보안 및 옵저버빌리티 도구가 더욱 발전해야 한다는 것을 분명히 알 수 있습니다.

3. 사각지대를 제대로 인지하지 못하고 있으며 암호화된 트래픽의 위험에 대한 오해가 존재합니다.

알려지지 않은 사각지대가 많은 CISO에게 골칫거리를 안겨주고 있지만 동시에 IT 및 보안 리더의 **70%** 이상이 암호화된 데이터가 자유롭게 이동하도록 허용하고 있음을 인정합니다. 하이브리드 클라우드 사각지대를 구성하는 요소, 그리고 데이터가 암호화되었거나 내부에서만 이동한다는 이유로 데이터를 분석하지 않을 때 발생하는 위험과 관련해 전 세계가 그 심각성을 인지하지 못하고 있습니다.

4. CISO의 1/3은 가장 민감한 데이터가 어떻게 보호되고 있는지 잘 알지 못합니다.

CISO와 CIO는 최신 하이브리드 클라우드 환경에서 많은 어려움을 마주하고 있습니다. 그중 하나는 가장 중요하고 민감한 데이터가 어떻게 저장 및 보호되고 있는지에 대한 기본적인 지식이 부족하다는 것입니다. 이러한 옵저버빌리티의 부재는 중대한 가시성 격차로 인한 조직 내 위험 증가를 암시하는 예시 중 하나입니다.

5. IT 부서 간 협업은 아직 요원합니다.

협업이 증가하고 있습니다. 대다수는 클라우드 보안에 대한 책임이 모두에게 있으며 CloudOps와 SecOps가 공통의 목표를 향해 나아가고 있다고 답했습니다. 하지만 SecOps팀이 취약성 탐지를 위해 수고로운 작업을 수행하고 있다는 것을 아는 응답자의 **99%**는 실제로는 보안 우선 문화의 부재가 여전히 사일로를 생성하고 있다고 말했습니다.

6. 딥 옵저버빌리티는 클라우드 보안, 클라우드 비용 증가, 제로 트러스트의 핵심입니다.

2022 Gigamon 랜섬웨어 현황 및 그 이후 보고서의 결과에 이어 올해 수집한 데이터에서는 딥 옵저버빌리티가 하이브리드 클라우드 시장에서 보안과 관련해 빠르게 주목받고 있으며 제로 트러스트와 같은 보안 프레임워크의 기본 요소로 자리 잡고 있음을 강조합니다.[4] 또한 많은 이들이 어려운 경제 상황 속에서 딥 옵저버빌리티가 비용 효율성에 제공하는 이점을 목격하고 있습니다.

IT 협업의 증가

2022 Gigamon 랜섬웨어 현황 보고서 발표 이후 1년간 전 세계적으로 대규모 데이터 침해 사건이 다수 발생했습니다. 여기에는 글로벌 언론사, 학교, 통신업체 및 의료기관에 대한 공격이 포함됩니다. 이에 따라 기업 이사회뿐만 아니라 정부 기관도 사이버 보안을 주요 논의 주제로 삼기 시작했습니다. 최근 미국 백악관은 2021년 행정 명령(14028)에 이어 향후 10년간 미국 보안 전략의 중심이 될 가능성이 높은 새로운 국가 사이버 보안 전략[5]을 발표했습니다.[6] 한편 나머지 국가를 살펴보면 호주에서는 2018년 제정된 주요 사회기반시설 보안법의 개혁이 진행 중입니다.[7] 또한 영국 COBRA 회의에서는 랜섬웨어를 주요 주제로 다루었으며[8] EU는 사이버 복원력법의 형태로 자체 업데이트 규정을 제안했습니다.[9]

기업에서는 위협 환경이 고조되면서 보다 높은 수준의 부서 간 IT 협업을 촉진하고 있습니다. 대다수의 전 세계 IT 및 보안 리더(**97%**)는 취약성 탐지 및 대응과 관련해 IT 조직 전반에 걸친 협업이 가능하다는 데 동의했으며 **83%**는 '공동 책임'에 기반한 보안 문화가 조성되어 있다고 답했습니다. 이는 전체 IT 조직이 보안 책임을 공유하는 문화를 의미합니다. 이러한 문화에 대한 자신감은 EMEA(**10명 중 1명**이 여전히 각 보안팀에 책임을 분할)보다 미국, 호주, 싱가포르의 전문가들에게서 잘 드러납니다.

이러한 사이버 환경의 어려움에도 불구하고 좋은 소식은 EMEA, APAC 및 미국 내 IT 및 보안 전문가의 **99%**가 CloudOps와 SecOps가 공통의 목표를 향해 나아가고 있다고 답했다는 것입니다. 이에 더해 클라우드 보안이 모두의 우선순위라고 답한 비율은 **96%**에 달했습니다.

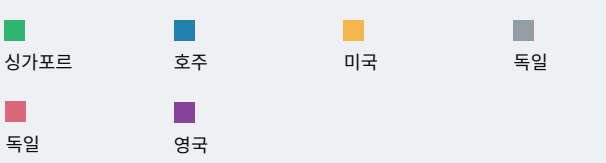
놀랍게도 응답자의 **69%**가 CloudOps가 조직의 보안 전략을 주도하고 사이버 공격을 방지한다고 답했습니다. 이는 SecOps가 동일한 역할을 수행한다고 답한 비율이 **53%**라는 사실에 의해 뒷받침됩니다. 싱가포르의 경우, 보안 전략 주도 측면에서 SecOps(**38%**)의 역할이 AppSec팀(**39%**)과 동등한 수준이라고 답한 비율은 약간 감소했지만 여전히 CloudOps(**59%**)는 핵심 부서로 강조되고 있습니다.

많은 CISO 및 고위 IT 보안 리더가 침해 발생 시 전적인 책임을 집니다. 귀하의 조직에서는 어떠한 유형의 보안 문화를 시행하고 있습니까?

고립된 책임 - CISO /대부분의 고위 보안 리더가 전적인 책임을 진다.

분할된 책임 – 각 보안팀이 책임을 진다.

공동 책임 - 전체 IT 조직이 책임을 공유한다.



이러한 사이버 환경의 어려움에도 불구하고 좋은 소식은 EMEA, APAC 및 미국 내 IT 및 보안 전문가의 **99%**가 CloudOps와 SecOps가 공통의 목표를 향해 나아가고 있다고 답했다는 것입니다.

하지만 중요한 사실은 협업을 강화하기 위해 필요한 일이 아직 많다는 것입니다. CloudOps팀이 전략을 주도하고 있지만 설문조사 결과는 SecOps 전문가들이 취약성 탐지를 '담당'하고 있음을 강조합니다. 무려 응답자의 **99%**가 보안 우선 문화의 부재로 인해 취약성 탐지 업무가 SecOps팀에 국한되는 경우가 많다고 답했습니다.

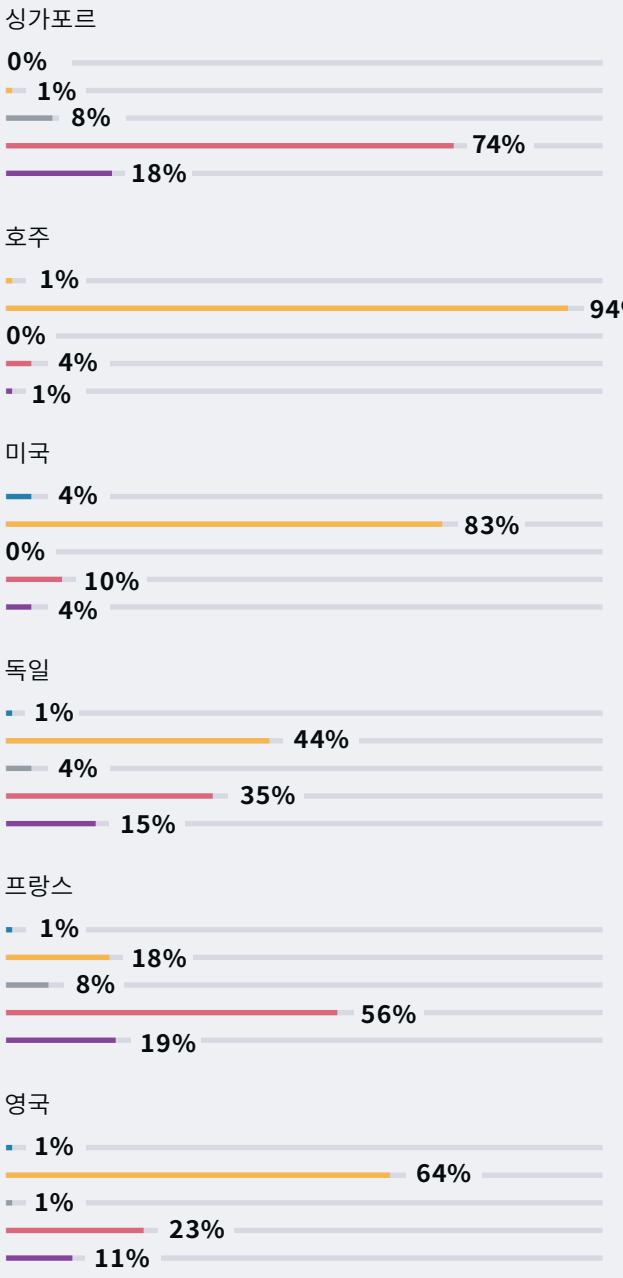
여전히 주요 관심사인 클라우드 보안

하이브리드 클라우드 인프라 보안과 관련한 위험 증가를 인지함에 따라 CloudOps와 SecOps 간 협업이 증가하고 있습니다. 최근 몇 년간 워크로드의 클라우드 전환은 많은 조직의 핵심 디지털 혁신 이니셔티브였습니다. 하지만 온프레미스용으로 설계된 대부분의 보안 및 모니터링 도구는 가상 또는 하이브리드 환경에 적합한 보호를 제공할 수 없습니다.

첫 번째 문제는 IT 리더십 사이에 클라우드 보안에 대한 완전한 합의가 이루어지지 않은 것처럼 보인다는 것입니다. 글로벌 CISO의 **30%**는 클라우드 마이그레이션 이니셔티브의 보안을 원하는 수준까지 안전하게 높일 수 있다는 완벽한 자신감이 있다고 답했지만 이러한 마이그레이션을 직접 수행하는 팀을 이끌 가능성이 높은 CISO에서는 대조적인 결과가 나왔습니다(완벽한 자신감이 있다고 답한 비율이 **12%**에 불과).

또한 이사회/CISO와 IT 및 보안 리더들 사이에 단절이 있는 것으로 보입니다. 이사회가 여전히 클라우드 책임 공유 모델을 이해하지 못한다고 답한 전 세계 응답자 비율이 절반 이상(**52%**)이라는 사실이 이를 더욱 심화시킵니다. 호주 IT 및 보안 리더의 **95%**와 미국의 **87%**가 이사회에게 모델에 대한 완벽한 이해가 없다고 답한 것이 이러한 결과의 주요 원인입니다. 반면 프랑스와 싱가포르는 더 높은 자신감을 보였습니다. 이와 같은 이해 부족은 우려를 야기하는 위험 요소인 동시에 클라우드 보안 책임에 대한 전 세계 의사결정권자들의 인식이 반드시 현실과 일치하는 것은 아님을 강조합니다.

클라우드 기반 보안 위협의 증가세를 고려할 때 이사회가 클라우드 고유의 책임 공유 모델을 완벽히 이해하고 있다는 데에 얼마나 동의합니까?



또한 이사회/CISO와 IT 및 보안 리더들 사이에 단절이 있는 것으로 보입니다. 이사회가 여전히 클라우드 책임 공유 모델을 이해하지 못한다고 답한 전 세계 응답자 비율이 절반 이상(52%)이라는 사실이 이를 더욱 심화시킵니다.

IT 및 보안 리더의 **93%**는 향후 12개월 동안 클라우드 보안 공격의 증가를 예상한다고 답했습니다. 이들의 과거 경험을 고려할 때 이러한 예측에 의문을 제기하기는 어렵습니다. 지난 18개월 동안 데이터 침해를 경험한 비율은 **90%**, 지난 7~9개월 동안 사이버 공격의 성공으로 어려움을 겪은 비율은 **59%**에 달했습니다.

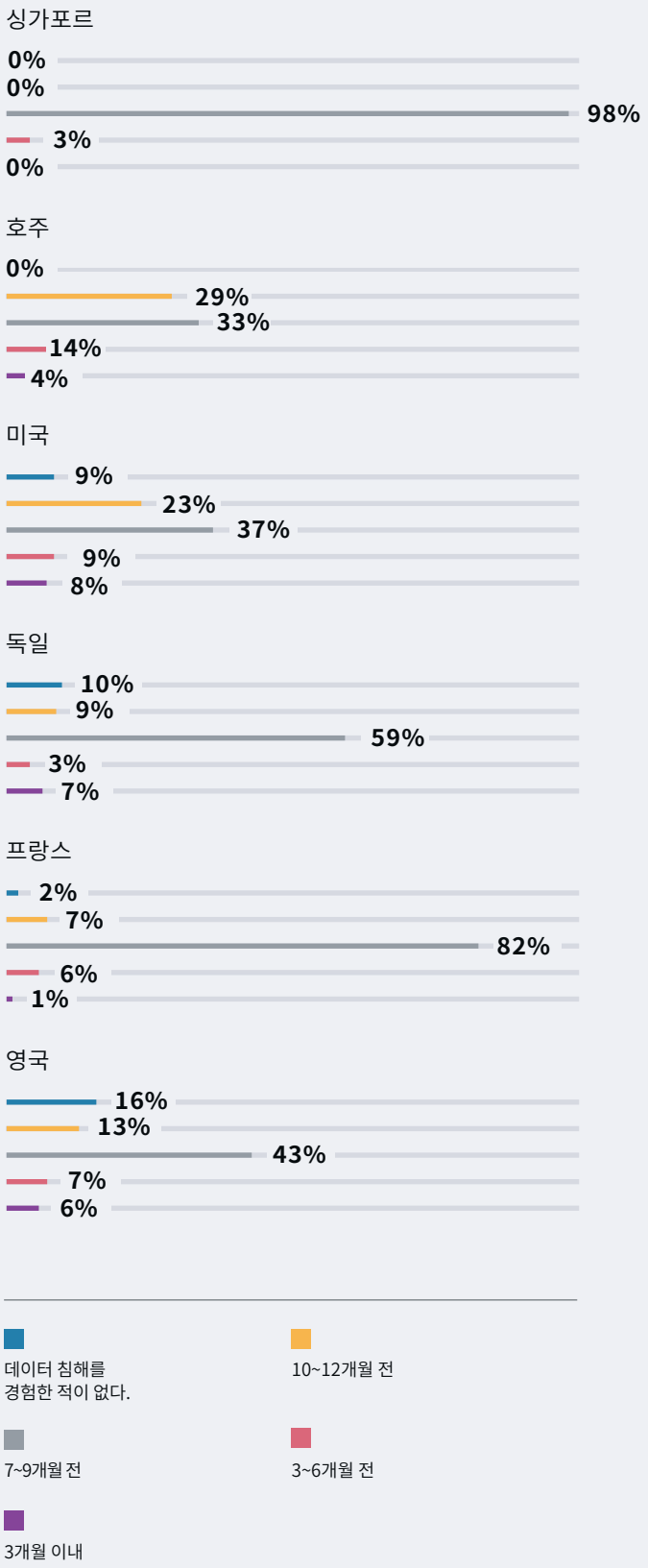
즉, 이들 팀은 가시성 보장에 필요한 적절한 수준의 협업을 구현했다는 점에는 동의할 수 있습니다. 하지만 하이브리드 클라우드 인프라 보안에 완벽히 자신있다고 답한 비율은 **16%**에 불과합니다. 여기에서 우리는 인식과 현실의 격차를 확인할 수 있습니다. 표면적인 자신감은 높지만 심층적인 조사에 들어가자 전문가가 완벽히 인지하거나 인지하지 못하는 다양한 문제 및 클라우드 보안 우려가 드러났습니다.

IT 및 보안 리더의 **93%**는 향후 12개월 동안 클라우드 보안 공격의 증가를 예상한다고 답했습니다. 이들의 과거 경험을 고려할 때 이러한 예측에 의문을 제기하기는 어렵습니다. 지난 18개월 동안 데이터 침해를 경험한 비율은 **90%**에 달했습니다.

이러한 현상은 전 세계적으로 나타나고 있지만 싱가포르 응답자들에게서 가장 확실하게 확인할 수 있었습니다. 1/4(**26%**)이 넘는 IT 및 보안 리더가 전체 IT 인프라 보안에 대해 완벽한 자신감이 있다고 답했으나('자신감'이 있다고 답한 비율은 **66%**) 이들 모두 지난 9개월 동안 침해를 경험했습니다. 프랑스의 경우, 온프레미스에서 클라우드에 이르는 IT 인프라 전반에서 충분한 보안을 구현하고 있다는 자신감 또는 완벽한 자신감이 있다고 답한 비율이 **81%**로 나타나며 싱가포르의 뒤를 바짝 쫓았습니다. 독일은 **55%**로 다소 낮은 수치를 보였습니다. 자신감이 더 낮게 나타난 국가는 영국(**36%**), 호주(**18%**), 미국(**17%**)뿐이었습니다. 이러한 결과는 이전에 취약했던 조직이 마지막 공격을 겪은 이후 보안 강화를 위해 상당한 변화를 겪었기 때문일 가능성이 높습니다. 동시에 현재 하이브리드 클라우드 보안에 안주하는 데 따르는 위험을 강조합니다.

클라우드 보안이 이동 중인 모든 데이터 전반에 걸친 가시성 확보에 달려 있다고 답한 응답자의 **96%**에 따르면 정답은 온프레미스에서 클라우드까지 보다 심층적인 옵저버빌리티를 달성하는 데 있습니다.

작년 한 해 데이터 침해를 경험한 적이 있습니까?



가시성 격차로 어려움을 겪고 있는 보안팀

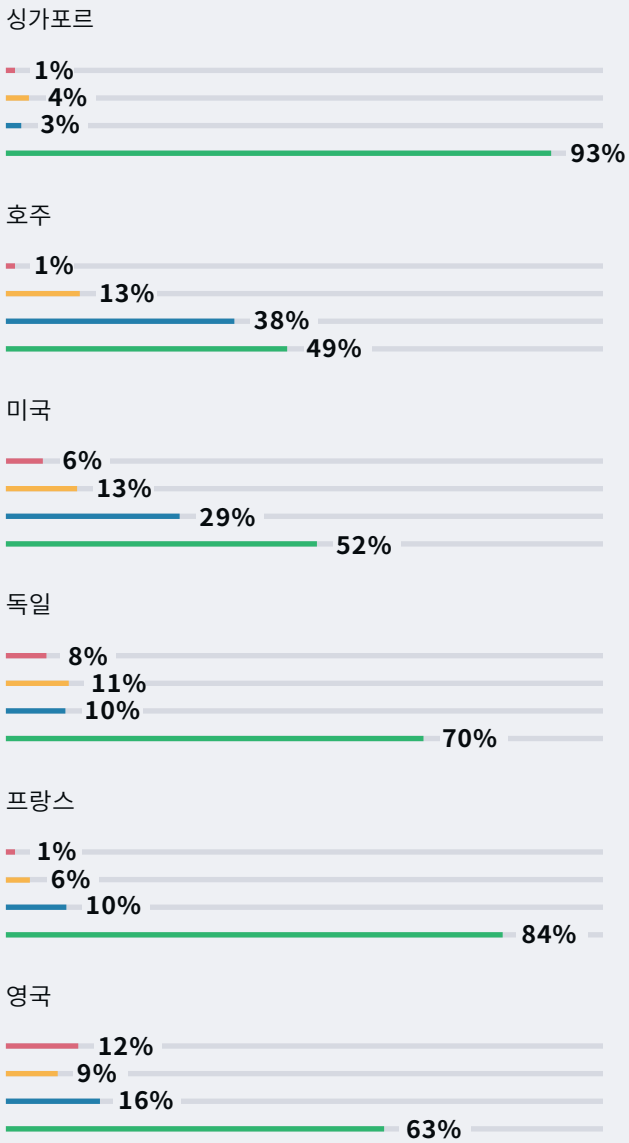
가시성이 하이브리드 클라우드 보안 문제를 해결할 수 있는 핵심 요소로 언급되고 있음에도 불구하고 많은 이들이 가시성 확보에 어려움을 겪고 있습니다. 가장 우려스러운 점은 침해를 경험한 적이 있는 전 세계 응답자들에게 침해를 정확히 어떻게 탐지했는지 물었을 때 보안 및 옵저버빌리티 도구를 이용한 비율은 **69%**에 불과했다는 것입니다. 나머지 **31%**는 다음과 같이 답했습니다.

- (DoS 또는 전송 중 유출 등으로 인해) 사용자가 애플리케이션 성능 지연을 경험했다(**18%**).
- 사용자가 애플리케이션 및 디지털 리소스 액세스에 실패했다(**9%**).
- 조직의 독점 정보가 다크웹에 유출되었다(**4%**).

이러한 결과는 IT 및 보안 전문가들과 이들이 사용하는 도구가 보안 침해의 약 **1/3**을 탐지하지 못하고 있음을 강조합니다. 해당 비율은 미국에서는 **48%**, 호주에서는 **52%**로 증가하며 우려를 야기하고 있습니다. 또한 EMEA에서는 약 **1/5**(**18%**)이 조직에서 발생한 침해의 근본 원인을 식별할 수 없다고 답했습니다.

글로벌 IT 및 보안 리더의 **50%**는 가장 민감한 데이터가 어디에 저장되고 어떻게 보호되는지 확실히 알지 못한다고 답했습니다.

데이터 침해를 어떻게 탐지했습니까?



가시성 격차가 침해 탐지 및 공격 후 문제 시정 과정에서 많은 문제를 야기하는 것으로 보입니다. 추가 공격 방지를 위한 하이브리드 클라우드 전반의 옵저버빌리티 수준에 대해 질문했을 때 더욱 우려스러운 결과가 나타났습니다.

글로벌 IT 및 보안 리더의 **50%**는 가장 민감한 데이터가 어디에 저장되고 어떻게 보호되는지 확실히 알지 못한다고 답했습니다. 이는 또한 이러한 지식에 대해 자신감을 보인 CISO/CIO가 **1/3**에 불과함을 강조합니다.

표면적으로는 보안 도구 및 프로세스가 하이브리드 클라우드 인프라에 대한 완벽한 가시성 및 인사이트를 제공한다고 답한 응답자 비율이 **94%**로 나타나지만 현실에서는 가장 중요한 데이터의 저장 방식 및 위치 또는 보호 방식을 잘 알지 못하는 경우 전략은 실패로 끝납니다.

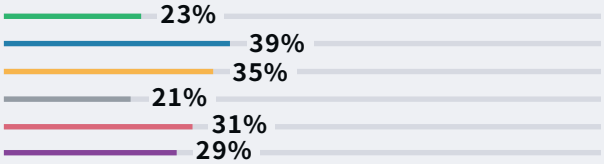
하이브리드 클라우드 인프라 전반에 걸친 가시성 수준에 대한 세분화된 질문을 통해 다음과 같은 사실을 발견했습니다.

- **35%**는 우수한 네트워크 가시성 대비 컨테이너 가시성이 제한적이라고 답했습니다(프랑스에서는 **38%**, 싱가포르에서는 **43%**로 증가).
- 암호화된 데이터에 대한 가시성을 확보한 비율은 **30%**에 불과했으며 독일에서는 **21%**로 더 낮았습니다.
- 절반 미만(**48%**)이 측면 이동 데이터 즉, 동서(East-West) 트래픽에 대한 가시성을 보유하고 있다고 답했습니다. 동서 가시성을 확보한 비율이 **64%**로 나타난 미국이 이 부문을 선도하고 있으며 싱가포르는 **30%**로 낮은 수치를 보여줍니다.

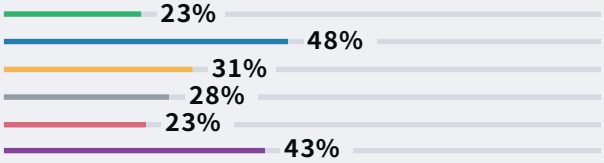
Gigamon의 보안 CTO 이안 파쿠하(Ian Farquhar)는 동서 가시성의 '재정의'가 필요하다고 말합니다. 동서 트래픽 vs. 북남(North-South) 데이터라는 기존 개념은 현재 하이브리드 클라우드 환경에 적용되지 않는 경계 중심 온프레미스 네트워크와 관련됩니다 오늘날의 최신 인프라에서는 측면 이동 데이터 전반에 걸친 딥 옵저버빌리티가 외부 소스에서 유입되는 트래픽에 대한 가시성만큼이나 중요합니다."

현재 IT 인프라 전반의 가시성 수준은 어떠합니까?

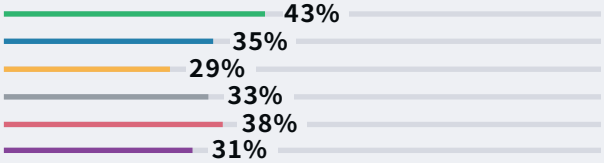
암호화된 데이터에 대한 가시성



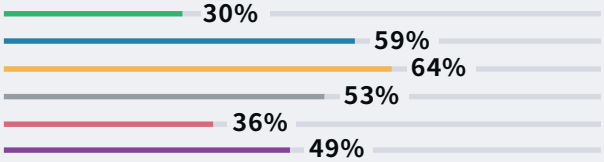
네트워크 레벨부터 애플리케이션 레벨까지의 가시성

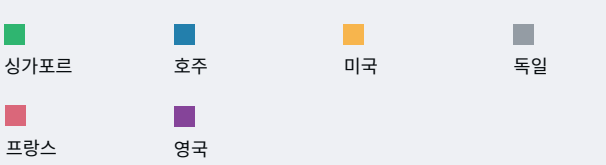


우수한 네트워크 가시성 대비 제한적인 컨테이너 레벨 가시성



동서(East-West) 가시성(측면)





동서 트래픽 vs. 북남(North-South) 데이터라는 기존 개념은 현재 하이브리드 클라우드 환경에 적용되지 않는 경계 중심 온프레미스 네트워크와 관련됩니다. 오늘날의 최신 인프라에서는 측면 이동 데이터 전반에 걸친 딥 옵저버빌리티가 외부 소스에서 유입되는 트래픽에 대한 가시성만큼이나 중요합니다.

이안 파쿠하
Gigamon 보안 CTO

응답자의 **56%**는 발견하지 못한 사각지대의 악용이 주요한 불안 요소라고 답했습니다.

이러한 결과는 대다수의 IT 및 보안팀이 온프레미스에서 클라우드로 이동 중인 데이터에 대한 핵심적인 가시성이 부족하지만 '사각지대'라는 인식이 없기 때문에 이를 문제로 인지하지 못할 수도 있음을 보여줍니다.

사각지대는 보안 및 모니터링 도구가 도달할 수 없는 네트워크 및 클라우드 전반의 세그먼트로 정의됩니다. 충분한 데이터 분석이 불가능해 해당 영역은 겉으로 드러나지 않습니다. 보안 및 모니터링 도구는 일반적으로 북-남 트래픽(외부에서 내부로 유입)만큼 중대한 위협으로 인식되지 않는 동서 트래픽(조직 내 측면 이동 데이터)을 무시할 수 있습니다. 암호화된 트래픽도 마찬가지입니다. 암호화 뒤에 숨겨진 **93%**의 멀웨어가 확인된 연구 결과에도 불구하고 조직은 이 데이터가 초래할 수 있는 큰 위험을 인식하지 못하고 있을 가능성이 있습니다.[10]

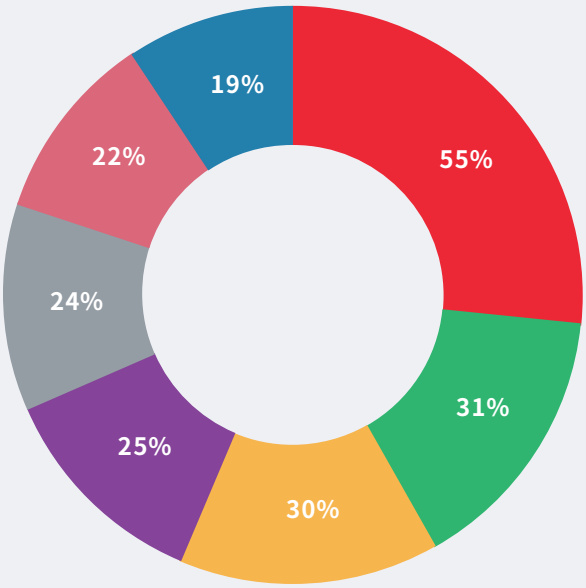
CISO에게 고민을 안겨주는 예상치 못한 문제들

이러한 상황을 고려할 때 CISO, CIO 및 기타 IT 및 보안 리더들의 가장 큰 고민거리가 사각지대라는 사실은 놀랍지 않습니다. 실제로 응답자의 **56%**는 발견하지 못한 사각지대의 악용이 주요한 불안 요소라고 답했습니다.

프랑스에서는 이 문제에 대해 우려하는 비율이 낮게 나타났습니다. 사각지대가 여전히 스트레스를 안겨주는 대표적인 요인이지만 이 때문에 고민한다고 답한 비율은 **36%**에 불과했습니다. 특히 영국의 경우, **40%**가 조직의 적절한 보안을 위한 도구/가시성의 부재에 대한 우려가 있다고 답했습니다.

또 하나의 놀라운 결과는 전통적으로 주요 고충점으로 간주되며 최근 몇 년간 헤드라인에서 자주 보이는 문제들이 2023년에는 IT 및 보안 리더의 주요 우려 사항이 아니라는 점입니다. 사각지대와 함께 법률(**34%**) 및 공격의 복잡성(**32%**)이 대표적인 스트레스 요인이었으며 사이버 투자 부족(**14%**) 및 지속적인 기술 격차(**20%**)와 같은 문제는 그 비율이 훨씬 낮았습니다. 프랑스에서는 다시 한번 예외적인 결과가 나타났는데 응답자의 1/4 이상(**26%**)이 부족한 사이버 보안 투자가 우려된다고 답했습니다.

오늘날의 환경에서는 사이버 인시던트에 대한 CISO와 고위 IT 보안 리더의 책임이 큰 주목을 받고 있습니다. 요즘 주된 우려 사항은 무엇입니까?



- 인지하지 못한 사각지대의 악용
- 증가하는 공격의 정교함 및 복잡성
- 조직의 보안에 필요한 도구/가시성 부재
- 불충분한 사이버 보안 투자
- 보다 집중적이고 중대한 신규 사이버 보안 법률
- 이사회의 압력
- 숙련된 사이버 보안 인력 부족(기술 격차)

실제로 하이브리드 클라우드 보안에서 기술을 거의 고려하지 않는 것이 전 세계적인 추세입니다. 직원들을 대상으로 한 효과적인 보안 교육이 자신 있는 IT 인프라 보안을 위해 필수라고 답한 비율은 **19%**에 불과했습니다. 또한 숙련된 클라우드 인력이 필요하다고 답한 비율은 **15%**였습니다. 프랑스와 독일에서만 기술 격차 감소가 높은 우선순위에 있는 것으로 보입니다. 하이브리드 클라우드 인프라가 최대한 안전하다는 자신감을 확보하는 데 숙련된 클라우드 인력이 중요하다고 답한 비율은 각각 **23%**와 **25%**였습니다.

한편 영국과 호주에서는 특별히 법률의 발전이 문제로 나타나고 있습니다. 영국 IT 및 보안 리더의 **41%**, 호주의 **59%**가 사이버 법률 및 규정 준수의 변화가 향후 최대 관심사라고 답했습니다. EU 사이버 복원력법이 전 세계적으로 가장 큰 고민을 야기하는 것으로 보입니다. 규정 미준수가 더욱 심각한 결과로 이어지는 오늘날(EU의 디지털 운영 복원력법이 벌금 또는 징역형 규정) 보안 리더들은 법률의 변화에 더욱 주의를 기울이고 있습니다.

글로벌 기업 중 ChatGPT를 금지했거나 금지를 고려하고 있는 비율은 **24%**였으며 TikTok/메타버스에 대해 우려를 표명한 비율은 **100%**였습니다. 실제로 글로벌 기업의 **60%**는 이미 사이버 보안에 대한 우려로 인해 WhatsApp 사용을 금지했습니다. 이 수치는 독일에서는 **67%**, 프랑스에서는 **69%**로 더 높게 나타났습니다.

사이버 보안 문제로 인해 조직에서 다음 앱, 도구 또는 기술을 사용하는 것에 대한 우려를 가지고 있습니까?

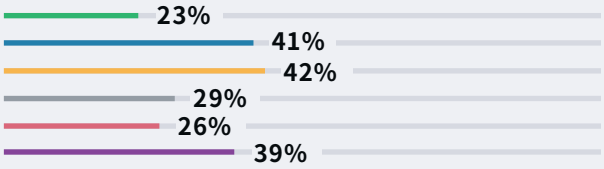
- 그렇다. 사이버 보안에 대한 우려로 인해 이미 사용을 금지했다.
- 그렇다. 현재 관련 사이버 보안 위험을 평가 중이며 곧 결정을 내릴 것이다.
- 아니다. 현재 사이버 보안에 대한 우려로 인해 사용을 금지할 계획이 없다.

마지막으로 AI가 중요한 위협이라는 보안 전문가들의 인식은 현실과 일치하지 않습니다. 올해 ChatGPT 및 기타 생성형 AI 기술이 연일 헤드라인을 장식했습니다. 하지만 당사 데이터에 따르면 글로벌 기업 중 ChatGPT를 금지했거나 금지를 고려하고 있는 비율은 **24%**였으며 TikTok/메타버스 및 WhatsApp에 대해 우려를 표명한 비율은 각각 **100%** 및 **99%**였습니다. 실제로 글로벌 기업의 **60%**는 이미 사이버 보안에 대한 우려로 인해 WhatsApp 사용을 금지했습니다. 이 수치는 독일에서는 **67%**, 프랑스에서는 **69%**로 더 높게 나타났습니다.

이러한 결과는 AI가 마음속에 가장 먼저 떠오르는 혁신 도구이지만 실제로 발전된 다양한 기술들이 사이버 리더들에게 고민을 안겨주고 있음을 의미합니다.

조직 전반에 걸친 묵시적 신뢰 제거 및 보안 대응 메커니즘 자동화를 목표로 하는 이 보안 프레임워크는 오래 전부터 전 세계 IT 및 보안 리더의 우선순위에 있었습니다.

현재 제로 트러스트를 뒷받침할 수 있는 네트워크, 시스템, 애플리케이션 전반에 걸친 가시성을 보유하고 있습니까?



보안 로드맵에 통합되는 제로 트러스트

제로 트러스트에서도 가시성 개선이 필요합니다. 조직 전반에 걸친 묵시적 신뢰 제거 및 보안 대응 메커니즘 자동화를 목표로 하는 이 보안 프레임워크는 오래 전부터 전 세계 IT 및 보안 리더의 우선순위에 있었습니다. 2022년에는 CISO/CIO의 **80%**가 제로 트러스트가 주요 트렌드가 될 것이라는 데 동의했으며(2022년 Gigamon 랜섬웨어 현황 보고서) 올해는 **96%**가 2023년 이후에도 이러한 추세가 이어질 것이라고 답했습니다.

반면 올해 설문조사의 전체 응답자 중 절반이 제로 트러스트가 조직이 안전하다는 확신을 갖는 데 중요하다고 답했지만 실제로는 구현에 필요한 가시성이 없는 팀이 많습니다. 이는 이사회가 제로 트러스트 이니셔티브를 촉진하고 있지만 변화를 직접 실행하는 이들이 아직 필요한 투자나 역량을 보유하고 있지 않기 때문일 수 있습니다.

당사 데이터에 따르면 제로 트러스트를 뒷받침하는 네트워크, 시스템, 애플리케이션 전반에 대한 가시성을 보유하고 있다고 답한 비율은 전 세계 응답자의 **34%**에 불과했습니다. 이 프레임워크를 구현하는 데 필요한 가시성 달성 측면에서는 영국(**39%**), 미국(**42%**) 및 호주(**41%**)가 시장에서 앞서고 있으며 프랑스(**26%**), 독일(**29%**), 싱가포르(**25%**)가 뒤를 이었습니다.

좋은 소식은 제로 트러스트에 수반되는 것에 대한 정확한 이해 및 인식이 높아지고 있다는 것입니다. 또한 제로 트러스트에 대해 이사회의 공개 논의도 증가 추세에 있습니다. 예를 들어, 영국에서 이사회가 제로 트러스트에 대해 논의한 적이 있다고 답한 비율은 2021년에 **53%**였으며 2022년에는 **67%**, 2023년에는 85%로 증가했습니다. 전 세계로 범위를 넓히면 이 수치는 작년에 **58%**에서 **87%**로 증가했습니다. 또한 제로 트러스트를 단순한 행정 관행이 아닌 여정이라고 답한 비율은 2022년 3/4에서 2023년 **96%**로 증가했습니다.

제로 트러스트의 완벽한 달성이 불가능하다는 데에 얼마나 동의합니까?

하지만 당사의 작년 글로벌 랜섬웨어 보고서 결과에서 확인했듯이 제로 트러스트에 대한 이해도가 높아지면서 제로 트러스트의 복잡성 및 구현 현실을 둘러싼 회의론이 대두되고 있습니다. 정부 기관에서 충분한 지침이 발표되지 않아 많은 이들이 프레임워크 배포 방법에 여전히 확신을 갖지 못하고 있습니다. EMEA의 경우, 2021년에 제로 트러스트 달성이 가능하다고 답한 비율이 **77%**였지만 2022년에는 **53%**로 감소해 현재는 절반도 되지 않습니다(**44%**). 실제로 프랑스에서는 이러한 보안 접근 방식을 달성할 자신이 있다고 답한 비율이 **20%**에 불과했습니다.

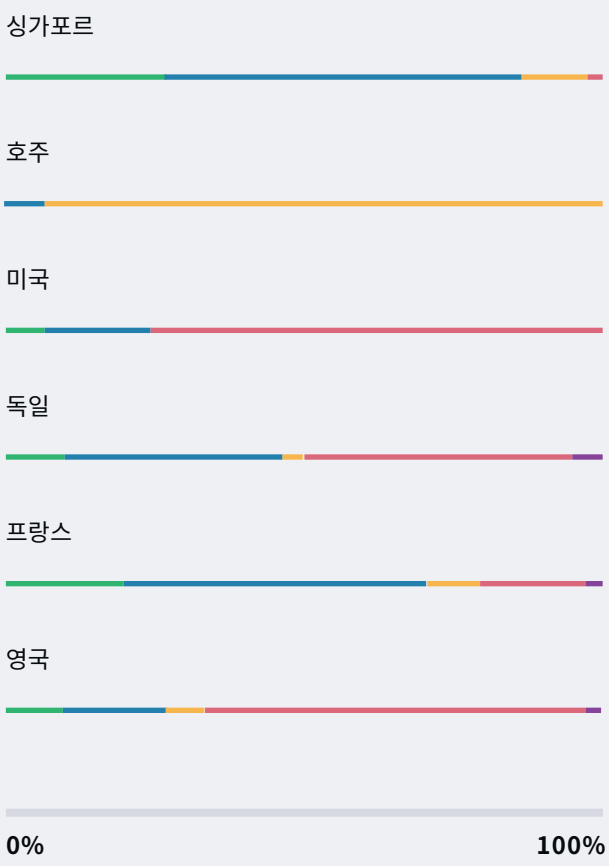
이처럼 제로 트러스트가 '달성 불가능'하다고 보는 의견은 긍정적인 결과를 얻기 위한 프레임워크 설계에 필요한 투자 수준이 반영된 결과일 수 있습니다. 2년 전에는 EMEA의 IT 및 보안 리더 중 **21%**만이 효과적인 제로 트러스트를 구현하는 데 너무 많은 인사이트와 리소스가 필요하다고 답했습니다. 하지만 이 수치는 프랑스에 퍼진 회의론에 힘입어(**76%**) 2022년에 **44%**, 2023년에는 **53%**로 증가했습니다.

전 세계적으로 결과에 큰 차이가 나타나고 있습니다. 일부 지역에서는 예전과 달리 제로 트러스트의 미래에 대한 자신감과 편안함이 더욱 높아진 것을 확인할 수 있습니다. 예를 들어, 호주에서는 제로 트러스트의 가능성에 대한 우호적인 태도가 훨씬 늘어났습니다. 2022년에 필요한 인사이트/리소스의 규모로 인해 투자할 가치가 없다고 답한 비율이 **48%**에서 현재 **7%**로 줄었습니다. 미국 역시 이와 유사하게 작년에 **21%**였던 회의적 태도가 올해 **12%**로 감소했습니다.

싱가포르와 프랑스에서는 다른 결과가 나타나고 있습니다. 싱가포르의 경우, 부정적인 태도가 가장 두드러졌습니다. **91%**가 제로 트러스트 달성이 불가능하다고 답했으며(2022년 대비 **63%** 증가) **96%**는 너무 많은 감독 활동이 필요하다고 답했습니다.

이러한 지역적 차이는 또한 제로 트러스트가 단순한 유행어에 불과한지에 대해 묻는 질문에 서로 다른 답변을 이끌어냈습니다. 응답자의 **45%**는 이에 동의했고 **53%**는 동의하지 않았습니다. 호주와 미국에서 이러한 보안 접근 방식이 현실적이고 달성 가능하다는 의견을 뒷받침하는 결과가 나온 반면 싱가포르와 프랑스는 여전히 확신이 부족합니다.

제로 트러스트가 실제가 아닌 유행어에 가깝다는 점에 얼마나 동의합니까?



그 어느 때보다도 커진 딥 옵저버빌리티의 가치

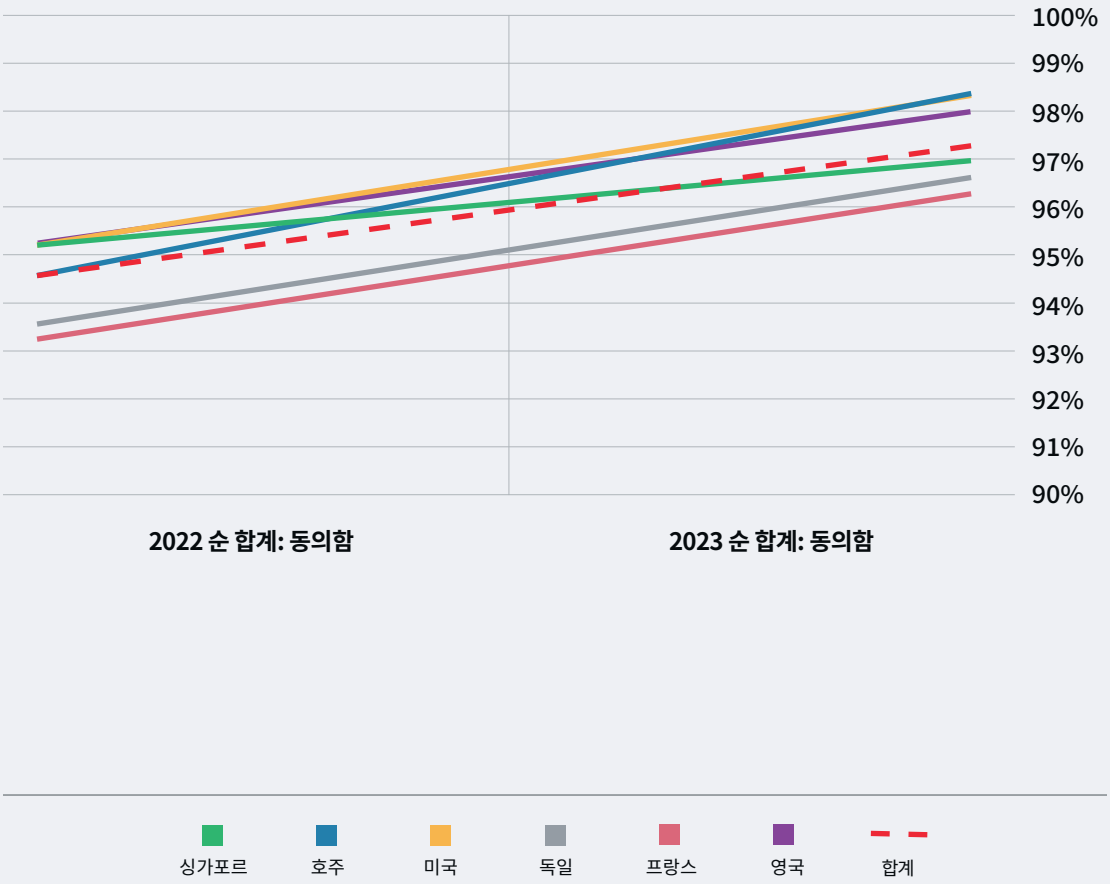
제로 트러스트를 둘러싼 불확신성은 이 프레임워크의 실제 작동 방식에 대한 이해 부족에서 기인할 가능성이 높습니다. 이안 파쿠하에 따르면 진정한 제로 트러스트 프레임워크는 여전히 '진행 중'입니다. 그는 "보안팀은 제로 트러스트 아키텍처 구현 과정에서 이것이 단순한 솔루션이 아님을 빠르게 깨닫고 있다. 특히 미국이 행정 명령 14028을 통해 연방 기관의 제로 트러스트 구현을 의무화하면서 많은 조직이 계속해서 제로 트러스트 여정을 진행 중이다. 우리는 제로 트러스트가 보안 전략의 구성 요소이자 비즈니스 민첩성 유지와 동시에 보안 복원력의 획기적인 개선을 위한 최상의 선택지임을 분명히 알 수 있다"고 주장했습니다.

다행히 이번 설문조사에 참여한 모든 IT 및 보안 전문가는 어디에서부터 제로 트러스트를 위한 견고한 토대를 구축해야 할지 잘 알고 있는 것으로 보입니다. 딥 옵저버빌리티와 제로 트러스트가 강력한 연관성이 있다고 답한 비율은 2022년에는 **89%**였지만 2023년에는 **100%**로 증가했습니다.

이는 온프레미스용으로 설계된 전통적인 로그 기반 도구를 넘어 전 세계 IT 및 보안 리더가 이번 설문조사 결과에서 강조한 중대한 가시성 격차에 대해 실행 가능한 네트워크 유래 인텔리전스를 제공하는 딥 옵저버빌리티로 인한 것일 가능성이 높습니다. 딥 옵저버빌리티는 상대적으로 최근에 등장한 용어이지만 하이브리드 클라우드 인프라 보안과 관련해 특히 그 가치를 빠르게 인정받고 있습니다. 당사는 2022년 설문조사 응답자들에게 딥 옵저버빌리티에 대한 상세한 정의를 제공했고 이것이 클라우드 보안의 중요 요소라는 것에 **89%**가 동의했습니다. 2023년에는 이 수치가 **97%**로 증가했습니다. 또한 이사회가 딥 옵저버빌리티를 하이브리드 클라우드 보안 개선을 위한 우선순위로 논의하고 있다고 답한 비율도 작년보다 **20%** 증가하며 **98%**에 달했습니다.

> 진정한 제로 트러스트 프레임워크는 여전히 '진행 중'입니다. 보안팀은 제로 트러스트 아키텍처 구현 과정에서 이것이 단순한 솔루션이 아님을 빠르게 깨닫고 있습니다. 특히 미국이 행정 명령 14028을 통해 연방 기관의 제로 트러스트 구현을 의무화하면서 많은 조직이 계속해서 제로 트러스트 여정을 진행 중입니다. 우리는 제로 트러스트가 보안 전략의 구성 요소이자 비즈니스 민첩성 유지와 동시에 보안 복원력의 획기적인 개선을 위한 최상의 선택지임을 분명히 알 수 있습니다.
>
> **이안 파쿠하**
> Gigamon 보안 CTO

딥 옵저버빌리티가 클라우드 보안의 기본 요소라는 점에 얼마나 동의합니까?



마지막으로 딥 옵저버빌리티는 하이브리드 클라우드 인프라 보안뿐만 아니라 비용 관리와 관련해서도 언급됩니다. 예상치 못한 클라우드 컴퓨팅 비용 상승이 중대한 방해 요소가 되었다는 것은 이제 널리 알려진 사실입니다. 하지만 하이브리드 클라우드 가시성 개선은 관련 트래픽만 관련 도구로 전송함으로써 상당한 에이전트, 대역폭 및 데이터 이동 비용 절감 효과를 제공합니다. 당사 연구에 따르면 딥 옵저버빌리티는 핵심 요소로서 하이브리드/멀티 클라우드 인프라 관련 보안 도구 비용을 효과적으로 관리할 수 있다는 자신감이 부족한 글로벌 IT 및 보안 리더와 팀의 **50%**를 지원할 것입니다.

본 보고서에서 강조하고 있는 사각지대를 고려할 때 딥 옵저버빌리티와 기존 보안 및 모니터링 도구의 개선을 통해 얻을 수 있는 가치에 대한 인식이 높아진 것은 긍정적인 현상입니다. 하이브리드 클라우드 보안의 개선은 많은 조직이 인식과 현실의 격차로 인해 어려움을 겪고 있다는 사실을 인지하는 것에서 시작됩니다. 현재 상태에 대한 만족은 취약성으로 이어질 수 있습니다. 본 보고서는 동서 트래픽부터 암호화된 데이터에 이르기까지 보다 큰 주의를 요구하는 다양한 영역을 강조합니다. 다행히 전 세계 IT 및 보안 리더가 이러한 문제의 심각성에 대한 진정한 이해를 보유하게 되면 딥 옵저버빌리티를 바탕으로 보다 쉽게 격차를 해소할 수 있을 것입니다.

Gigamon 소개

Gigamon은 실행 가능한 네트워크 유래 인텔리전스를 바탕으로 옵저버빌리티 도구의 기능을 극대화하는 딥 옵저버빌리티 파이프라인을 제공합니다. 이 강력한 조합은 IT 조직의 보안 및 규정 준수 거버넌스 보장, 성능 병목 현상의 근본 원인에 대한 신속한 분석 및 하이브리드/멀티 클라우드 IT 인프라 관리에 수반되는 운영 간접비 절감을 지원합니다. Gigamon은 이를 통해 오늘날의 기업들이 클라우드의 혁신 잠재력을 완벽히 구현할 수 있도록 합니다. Gigamon은 Fortune 100대 기업의 80% 이상, 10대 모바일 네트워크 공급업체 중 9개, 수백 개 이상의 정부 및 교육 기관을 포함한 전 세계 4,000여 고객에게 서비스를 제공하고 있습니다. Gigamon은 이를 통해 오늘날의 기업들이 클라우드의 혁신 잠재력을 완벽히 구현할 수 있도록 합니다. Gigamon은 Fortune 100대 기업의 80% 이상, 10대 모바일 네트워크 공급업체 중 9개, 수백 개 이상의 정부 및 교육 기관을 포함한 전 세계 4,000여 고객에게 서비스를 제공하고 있습니다. Gigamon 플랫폼에 대한 보다 자세한 정보 또는 현지 담당자 문의는 gigamon.com을 참조하십시오.

1 Forrester, Explore Seven Pitfalls To Avoid In Your Push To Modernize Cloud, https://www.forrester.com/resources/cloud-strategy/modernize- cloud-pitfalls-webinar/

2 Flexera, 2023 State of the Cloud Report, https://info.flexera.com/CM-REPORT-State-of-the-Cloud

3 Cisco, 2022 Global Hybrid Cloud Trends Report, https://www.cisco.com/c/en/us/solutions/hybrid-cloud/2022-trends.html

4 Gigamon, State of Ransomware for 2022 and Beyond, https://www.gigamon.com/resources/resource-library/white-paper/wp-gigamon- report-state-of-ransomware.html

5 The White House, National Cybersecurity Strategy, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet- biden-harris-administration-announces-national-cybersecurity-strategy/

6 The White House, Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential- actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

7 Cyber and Infrastructure Centre, Security of Critical Infrastructure Act 2018, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure

8 The Record, Ransomware incidents now make up majority of British government's crisis management 'Cobra' meetings, https://therecord. media/ransomware-incidents-now-make-up-majority-of-british-governments-crisis-management-cobra-meetings

9 European Cyber Resilience Act, https://www.european-cyber-resilience-act.com/

10 Help Net Security, The hidden picture of malware attack trends, https://www.helpnetsecurity.com/2023/04/06/malware-attack- trends-q4-2022/

Gigamon®

전 세계 본사
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.23_1