2022년 12월

2022년 물리 보안 현황:

변화하는 환경에 효과적으로 대응하는 방법

3,700명 이상의 물리 보안 전문가들의 연구 통찰

Genetec™

목차

연구에 대해

제네텍은 2022년 8월 24일부터 9월 21일까지 물리 보안 전문가를 대상으로 설문조사를 실시했습니다. 제출 자료에 대한 자료 점검과 검토를 거친 후 분석을 위해 3,711건의 응답지를 표본에 포함시켰습니다.

설문조사 방법에 대한 세부 정보

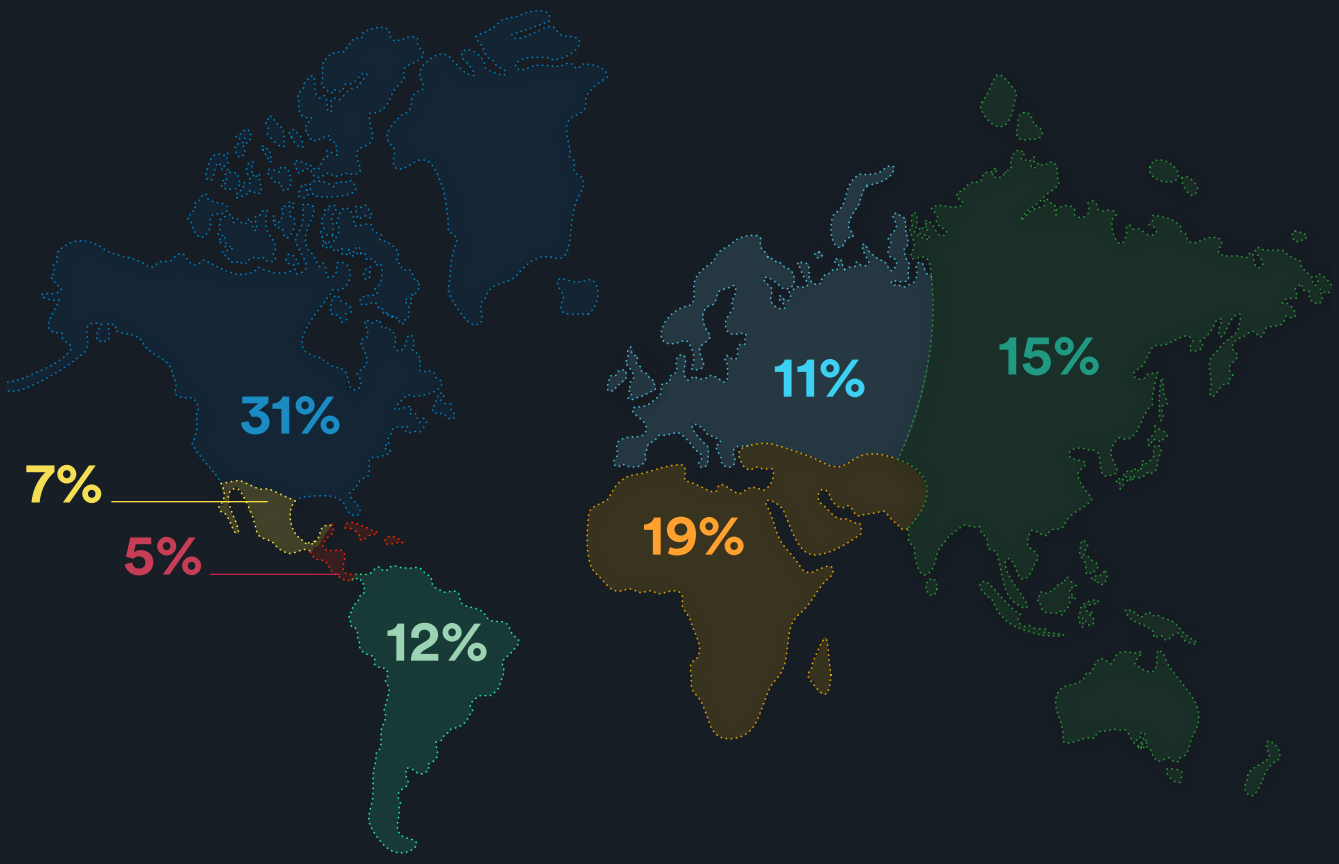
설문조사 대상 집단으로 다음 두 주요 집단에 초점을 맞추었습니다.

- 최종 사용자(물리 보안 기술을 조달, 관리 및 사용하는 기업에서 근무하는 개인)
- 시스템 통합(SI)과 시스템 설치업체 및 제공업체(보안 솔루션을 상담, 통합, 설치하거나 서비스하는 개별 업체)

대상 모집단은 타사가 수행한 제네텍 옵트인 이메일 목록 및 디지털 프로모션을 통해 선정되었습니다. 이 보고서의 일부 결과는 최종 사용자와 시스템 통합(SI)/시스템 설치업체/시스템 제공업체 모두의 응답을 기반으로 합니다. 하지만 일부 질문은 최종 사용자만을, 일부는 시스템 통합(SI)/시스템 설치업체/시스템 제공업체만을 대상으로 합니다. 이 보고서는 응답의 출처가 모든 응답자인지, 아니면 최종 사용자나 시스템 통합(SI)/시스템 설치업체/시스템 제공업체인지 표시합니다.

양 집단(최종 사용자 및 시스템 통합(SI)/시스템 설치업체/시스템 제공업체) 모두를 대상으로 한 질문에 대해서도 '최종 사용자만', '시스템 통합(SI)/시스템 설치업체/시스템 제공업체만', '두 집단 모두'를 구분해 결과를 분석했습니다. 대부분의 경우, 결과에 큰 차이는 없었습니다. 최종 사용자만의 응답이 시스템 통합(SI)/시스템 설치업체/시스템 제공업체의 응답과 거의 일치했던 것입니다. 보고서는 그에 해당되지 않는 경우에 대해 지적합니다. 또한 보고서는 지리적 지역, 최종 사용자의 산업 또는 전 세계 고용인 수로 측정한 기업 규모에 따라 응답 비율이 달라지는 경우를 강조합니다.

대상이 되는 모집단은 모든 지리적 지역에 걸쳐 표본으로 추출되었습니다.



최종 분석에는 대상 모집단에 속하는 개인이 빠짐없이 작성한 설문조사만 포함되었습니다.
설문조사 방법과 참가자의 인구통계학적 정보에 대한 자세한 내용은 부록 1과 부록 2를 참조하세요.

목차로 돌아가기

개요

COVID-19 팬데믹으로 인한 불확실성과 변화의 시간을 거친 기업들은 이제 새로운 업무 방식에 관심을 가져 이 방식에 정착하고 있습니다. 대부분의 2022년 설문조사 결과는 2021년 설문조사 응답과 여러모로 유사했습니다. 하지만 일부에서는 제품 품귀현상이나 인력 문제 등 업계가 직면한 새로운 난관이 드러났습니다.

기업들이 상황에 적응할 준비를 갖췄으며, 물리 보안 기술 도입에 대해 미래지향적이라는 점은 확실합니다.

클라우드의 미래는 하이브리드: 기업 다수는 인프라 투자를 최적화하고 하이브리드 방식을 이용해 비용 절감과 효율성 증대를 꾀하기 위해 온 프레미스 및 클라우드 기반 솔루션이 혼합된 형태의 물리 보안을 설치하고자 합니다.

사이버 보안과 IT의 영향: 사이버 우려로 인해 강력한 사이버 보안 전략을 도입하고 유지할 새로운 방식이 탄생하고 있습니다.

사업 운영 목적의 물리 보안 활용: 팬데믹으로 인해 많은 기업에서 복수의 시스템과 데이터 소스를 활용해 시설과 인적 동선을 관리하고 있습니다. 물리 보안 솔루션을 단순히 사람 및 자원 보호와 관련된 비용 이상으로 간주하는 경향은 지속될 것이며, 물리 보안 데이터를 활용하는 새로운 방식은 기업 및 운영 관련 의사결정에 있어서 더 많은 정보를 제공할 것입니다.

공급난 극복: 업계는 기존 하드웨어의 가치를 연장하거나 프로젝트 연기를 통해 공급난에 대응하고 있습니다. 컴포넌트가 준비되어 있기 때문에 보안 및 IT 부서들은 탄탄한 2023년도 예산을 바탕으로 설치를 완료하거나 신규 프로젝트를 시작하고자 합니다.

세계 각지의 차이점 요약

설문조사 질문 대부분에서 지역별 응답자 간 차이는 근소했습니다. 다시 말해, 지역별로 각 답안의 비율이 비슷했습니다. 이는 지난 한 해 동안 물리 보안의 발전 수준에 대한 시각이 전 세계적으로 일정해졌음을 드러냅니다.

다음은 특정 지역의 응답이 세계 평균과 크게 달랐던 사례입니다.

아시아태평양: 공급망과 클라우드

아시아태평양 지역 시스템 통합(SI)은 이듬해에 공급망 문제가 끼칠 영향에 대해 회의적입니다. **57.5%**는 공급망 문제가 "크게 증가"하거나 "다소 증가"할 것이라 대답했습니다. 이는 세계 평균인 **49%**를 웃도는 수치입니다.

응답자들에게 클라우드 도입이 오래 걸리는 이유에 순위를 매기도록 하였습니다. 종합적으로 "사이버 보안의 위험성 인식"이 가장 높은 평균 순위를 차지했습니다. 아시아태평양에서는 "데이터 손실 우려"의 순위가 가장 높았고, 근소한 차이로 "클라우드에 대한 이해 부족"이 뒤따랐습니다.

아시아태평양 지역에서는 프라이빗 클라우드 사용에서 앞서고 있습니다. 전 세계 응답자 대부분은 여전히 온 프레미스 스토리지 기기(NVR, 서버, NAS, SAN 등)에 영상을 저장합니다. 아시아태평양 지역 응답자의 **4.55%**는 영상 데이터를 "주로 프라이빗 클라우드"에 저장한다고 답했는데, 이는 그 어떤 지역보다도 높은 결과입니다.

중미: 융합 및 클라우드

중미 지역에서는 융합형 보안 시스템이 보편적이지 않습니다. "우리 기업의 VMS 및 출입통제 시스템은 연결되어 있지 않다(별개의 시스템이다)"가 두 번째로 많이 선택된 답이었습니다. 이 답은 나머지 모든 지역에서 가장 드물게 선택되었습니다.

중미 응답자들은 다른 지역보다 공용 클라우드 스토리지를 더 자주 이용한다고도 답했습니다. 중미 응답자의 **6.9%**는 "주로 공용 클라우드 스토리지 서비스에 저장"을 선택했으며, 나머지 국가들의 비율은 **2.6%**였습니다.

유럽, 중동, 터키, 아프리카: 클라우드, 크리덴셜 위협, 공급망

EMEA 지역은 물리 보안의 영역 내 리클라우드 도입에 관해서는 가장 보수적입니다. 글로벌 평균인 58%에 비해 이 지역 응답자의 69%가 보유 중인 인프라를 클라우드로 전혀 이전하지 않았다고 답했습니다.

"크리덴셜 도용"이 기업에게 가장 큰 위협이라고 답한 EMEA 지역 응답자는 50.2%에 달하며, 이는 글로벌 수치인 39.6%와 비교됩니다.

유럽은 지난 12개월 동안 프로젝트 수행에서 가장 큰 어려움을 겪었으며, 글로벌 평균인 71%에 비해 이 지역 응답자의 82%가 영향을 받았다고 답했습니다. 이는 예산 축소와 공급망 문제가 원인이라고 볼 수 있습니다. 이러한 난관에도 불구하고 응답자들은 대부분의 프로젝트가 취소되는 대신 2023년으로 연기되었다고 답했습니다.

멕시코: 클라우드

멕시코 응답자의 17.4%만이 COVID-19 로 인해 클라우드 전략이 어느 정도 가속화되었다고 밝혔습니다. 이는 글로벌 수치인 30.9%와 비교됩니다. 멕시코는 "다소" 또는 "크게" 가속화되었다고 답한 응답자의 비율이 가장 낮았는데(29.4%), 이는 글로벌 평균치인 46.7%나 미국 및 캐나다의 47.9%와 비교됩니다.

또한 멕시코에서는 COVID-19가 자신들의 클라우드 전략을 "촉발시켰다"고 답한 경우가 타 지역보다 많았습니다(9.8%). 같은 답을 한 미국 및 캐나다 내 응답자가 0.35%밖에 되지 않는 것(여러 지역 중 가장 낮은 수치)과는 뚜렷한 대조를 이룹니다.

남미: 원격근무 및 사이버 보안

남미 응답자의 50.4%는 자신의 기업 내에 직원의 원격근무가 가능하도록 설치된 물리 보안 조치가 없다고 답했으며, 해당 답변에 대한 글로벌 평균치는 33.7%였습니다.

또한 내년에 우선시할 신규 사안으로 "향상된 사이버 보안 전략"을 선택한 경우는 가장 적었습니다. 응답자의 단 38%만이 이 답안을 선택했는데, 이는 글로벌 평균인 49.2% 그리고 미국 및 캐나다의 52.9%와 비교됩니다.

미국 및 캐나다: 정리해고 감소, 온도 감지, 융합

미국 및 캐나다 응답자의 41%는 2021년에 해고된 보안 담당 직원이 "없다"고 답했습니다. 이는 글로벌 수치인 29%와 비교됩니다.

미국 및 캐나다 응답자들은 다른 지역에 비해 온도 감지 기술을 선택하는 비율이 낮았는데, 수치는 글로벌 평균인 24%과 대비되는 14%였습니다.

영상 및 출입통제 시스템 통합은 미국 및 캐나다에서 두 번째로 보편적이었으며, 글로벌 수치인 77%에 비해 응답자 중 80%가 융합형 시스템을 보유하고 있다고 답했습니다.

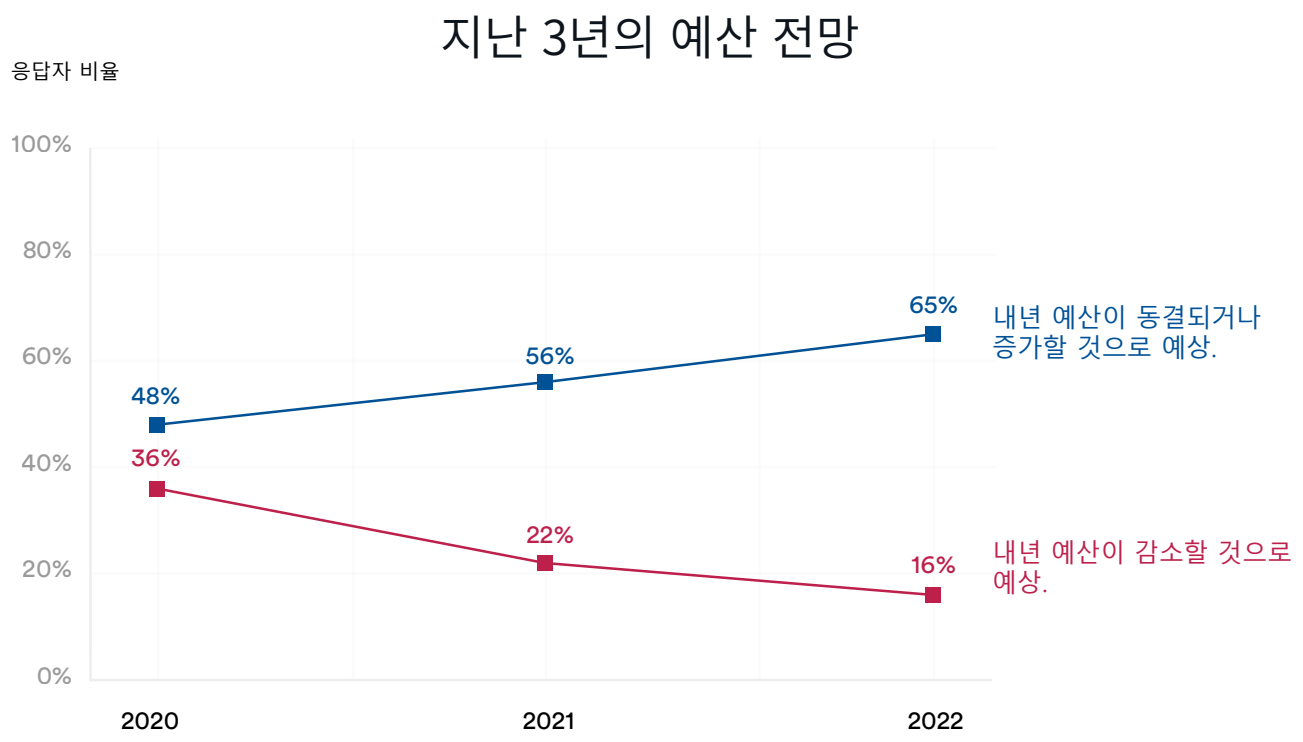
목차로 돌아가기

주요 결과

OPEX 예산 증가

여러 국가에서 경기 침체가 예측되고 있는 2023년의 암울한 경제 전망 속에서, 이전의 경기 후퇴 및 불경기 속에서도 물리 보안 시장은 지속적으로 증가했음에 주목하는 것이 중요합니다.
이러한 회복력은 설문 결과에도 반영된 것으로 보입니다. 2023년도 OPEX 예산에 대한 전반적인 전망이 긍정적이며, 팬데믹 시기의 결과로부터 회복세를 유지하고 있습니다.

OPEX 예산



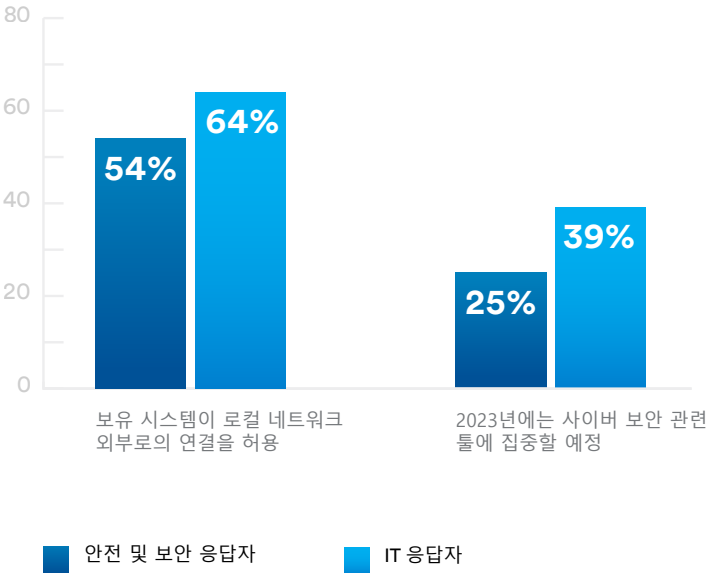
세계 각지의 경제 상황이 다름에도 불구하고 이 질문에 대한 답변은 지역별로 크게 다르지 않았습니다. 이는 물리 보안 업계 전반의 낙관적 시각을 반영합니다.

물리 보안 내 IT의 역할 증대

10년 전, 대기업에서 대부분의 물리 보안은 보안 전문 부서의 직원이 관리했습니다. 하지만 네트워크 물리 보안으로의 전환은 정보 기술(IT) 부서가 네트워크 및 기술 거버넌스의 일환으로 물리 보안 관리에 대해 더 큰 책임을 지게 된다는 사실을 의미했습니다. 2022년 설문에서 자신의 직무를 “정보 기술”로 답한 응답자가 “보안 및 안전성”을 선택한 이들과는 다른 관점을 보였던 것은 놀랍지 않은 일입니다. 네트워크 및 사이버 보안 문제는 이러한 물리 보안 시스템의 관리 및 설치와 관련 있는 “정보 기술” 응답자들의 답변에서 우선시되었습니다.

IT VS 보안

사이버 보안 도구의 우선순위화



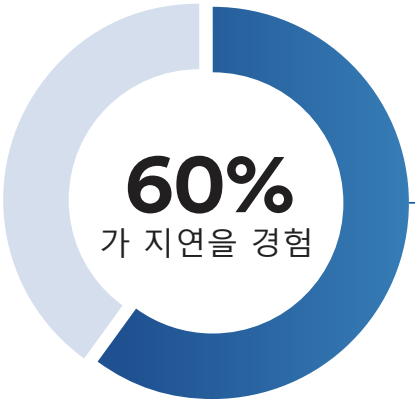
IT 분야 응답자는 랜섬웨어, 엔지니어링/피싱, 원격 공격을 기업의 최대 위협으로 보는 경향이 안전 및 보안 분야 응답자보다 높았습니다.

목차로 돌아가기

컴포넌트 경쟁

2021년에는 팬데믹으로 인한 규정과 제재가 존재했고, 대만 공장의 문제, 수에즈 운하 폐쇄, 통관항에서의 어려움 등이 발생했습니다. 업계 전반의 컴포넌트 수요가 크게 증가하고 (스마트폰 및 자동차 제조업체 등) 소비자의 "재택" 니즈가 새로 부상하면서 전에 없던 물리 보안 하드웨어 부족 현상과 프로젝트 지연 상황이 발생했습니다.

설문 결과는 만연한 공급망 문제의 영향과 이에 대해 물리 보안 실무자들이 취한 실용주의적 대응을 보여줍니다.



최종 사용자의 60%는 공급망 문제로 인해 물리 보안 프로젝트가 지연되었다고 답했습니다. 프로젝트 지연은 오래 지속되는 경우가 많았습니다.

- 최종 사용자의 46%는 3개월 이상의 프로젝트 지연을 경험했습니다.
- 최종 사용자의 28%는 6개월 이상의 프로젝트 지연을 경험했습니다.

다양한 유형의 프로젝트가 연기되었습니다. 프로젝트 지연을 겪은 최종 사용자 응답자들에게는 기술 또는 장비 대체가 가장 어려운 점이었고(66%), 현재 설치된 솔루션 확대(51%)와 업그레이드(51%)가 뒤를 따랐습니다.

VMS 하드웨어 공급업체들은 프로젝트 지연으로 인해 심각한 영향을 받았습니다. 최종 사용자의 45%가 대안을 찾아 브랜드를 바꿔가며 이용 가능한 장비를 설치했기 때문입니다.

시스템 통합(SI) 역시 하드웨어 품귀 현상에 대처하기 위해 "중고 장비"와 "고치기 쉬운 전자기기를 재사용하기 위한 수리 센터"를 활용하는 등 다양한 전략 시도가 필요했다고 밝혔습니다.

목차로 돌아가기

제네텍의 시각

COVID-19 위기와 이것이 하드웨어 및 전자기기 컴포넌트 가용성에 끼친 영향은 업계 대부분에서 공급망과 물류가 지닌 핵심적인 역할을 드러냈습니다.

팬데믹은 거의 끝났지만 새로운 사회경제적 상황과 현재의 지정학적 갈등으로 커진 불확실성이 세계 공급망에 지장을 주고 있습니다.

보안 업계에서는 시스템 통합(SI) 시 다음을 수행해야 합니다.

- 필요할 때 자재를 확보할 수 있도록 앞으로도 프로젝트 사전에 하드웨어를 주문
- 주문이 밀린 제품의 대안을 제공할 수 있는 협력업체와 긴밀한 관계를 형성
- 회복력과 적응력이 뛰어나고 원자재와 가용 컴포넌트를 바탕으로 제품을 신속하게 개량할 수 있는 공급업체와 협력

긍정적으로 보았을 때, 초기 지표들은 2023년에는 공급망 병목현상이 해소될 것이라고 암시하고 있습니다. 이는 적절한 시점에 신규 프로젝트에 착수하려는 시스템 통합(SI)에서 필요로 하는 상황일 것입니다.

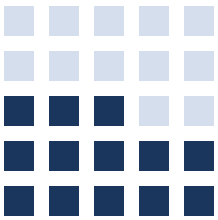
Nadia Boujenoui
고객경험 본부장
제네텍

인적 자원 관련 난관

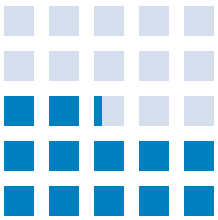
지난 2년 동안 모든 업계의 기업들은 인력 부족, 사무실 복귀 계획, 새로운 업무 방식에 대한 직원의 기대라는 문제를 겪었습니다.
물리 보안 업계도 크게 다르지 않았다는 사실이 설문 결과를 통해 드러났습니다.

2022년 설문 응답자의 50%는 자신들의 물리 보안 업체가 지난 해 인력 문제를 겪었다고 답했습니다. 응답자들은 이 문제로 인해
직원 교대 및 재배치를 해야 했고 이 상황에서 교육 비용이 제한적이었다고 밝혔습니다.

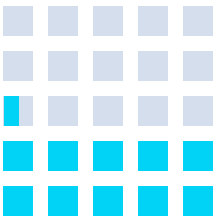
이러한 문제를 겪은 응답자 중:



52%
직원 부족 경험



49%
고용난 경험

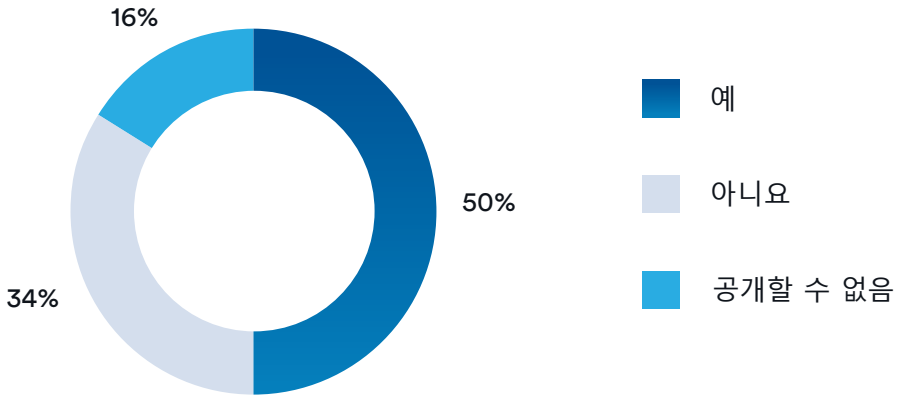


42%
직원 사기 문제 경험

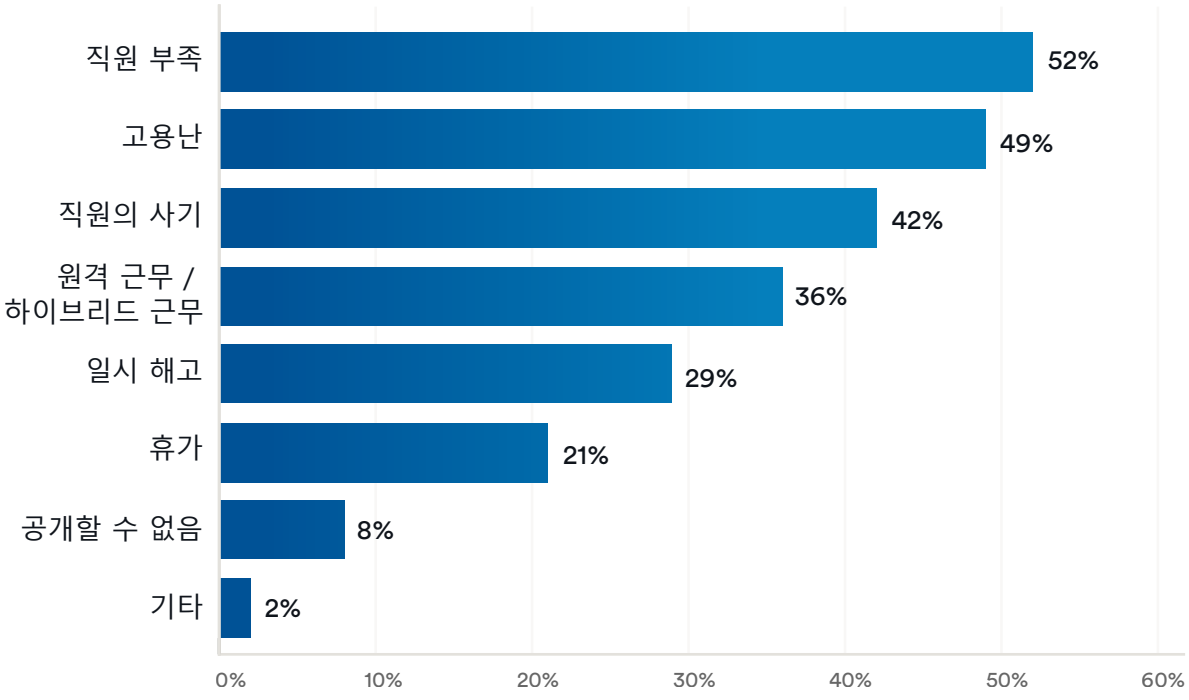
설문 결과 위 내용을 우선시한 48%의 응답자 중 83%는 대마, 73%는 게임 분야에 속했습니다.

인적 자원 관련 난관

귀하의 물리 보안 기업이 작년에 인력 문제를 경험한 적 있습니까?



지난 해 물리 보안 부서에 영향을 끼친 인력 문제는 무엇이었습니까?



목차로 돌아가기

클라우드 도입에 대한 관찰 사항

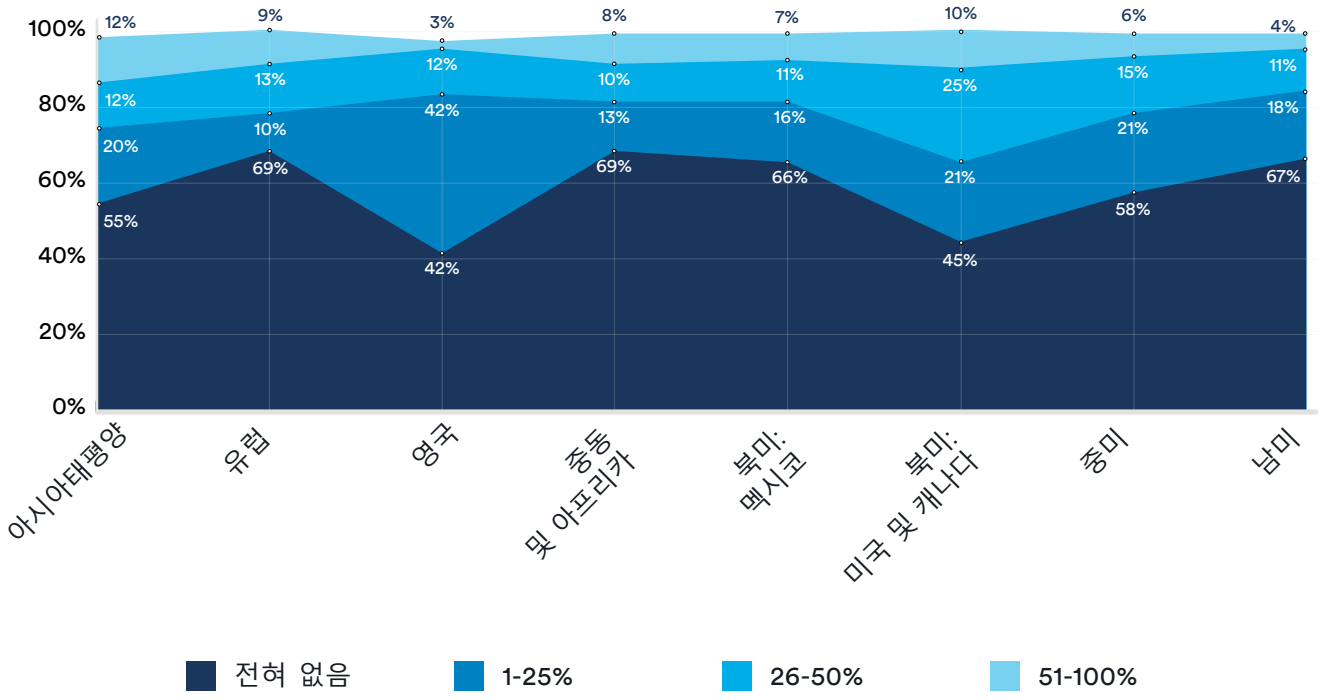
지역별 클라우드 수용도

최종 사용자 응답자의 대부분(82%)은 영상 자료를 온 프레미스 저장 기기(NVR, 서버, NAS, SAN 등)에 저장한다고 답했습니다. 단 6%만이 같은 용도로 공용이나 프라이빗 클라우드를 이용한다고 밝혔습니다. 가장 큰 이유는 원격 근무를 지원하기 위함이며, 이는 사무실에 상시 출퇴근하는 인원이 줄어들었기 때문에 타당해 보입니다.

유통 분야의 최종 사용자가 가장 높은 응답 비율을 보였는데, 응답자의 81%가 클라우드로 이전하겠다고 답했습니다. 또한 유럽 및 중동에서는 클라우드로 이전해 기업의 물리 보안 데이터를 관리 및 저장하겠다고 답한 응답자의 비율이 타 지역에 비해 낮았습니다.

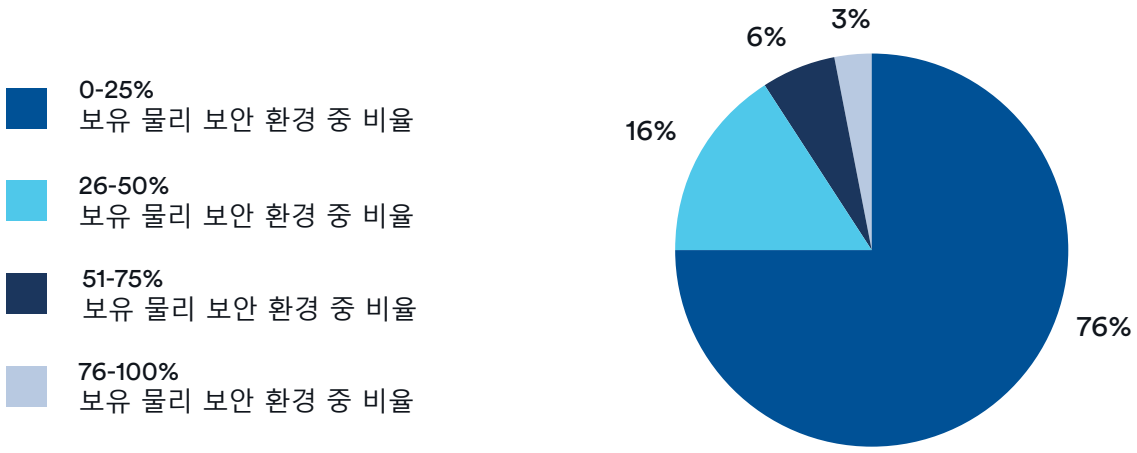
거의 2/3
전체 응답자 중 향후 2년간 클라우드에서 관리 및 저장하는 물리 보안 데이터의 양을 늘릴 계획이라고 답한 응답자의 비율.

지역별 클라우드 또는 하이브리드 클라우드 채택



목차로 돌아가기

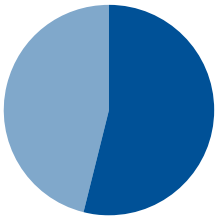
귀사에서 클라우드 또는 하이브리드 클라우드는 물리 보안 환경의 어느 정도를 차지하고 있습니까? (다음 중 택일)



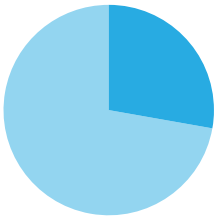
클라우드로의 이전은 업계 분석가의 예측과 일치합니다. Novaira Insights는 2021년에 19%였던 아메리카 대륙 내 클라우드 영상 관리 소프트웨어에서 발생하는 영상 관리 소프트웨어 매출 비율이 2026년에는 45%로 증가할 것이라고 보고했습니다.

목차로 돌아가기

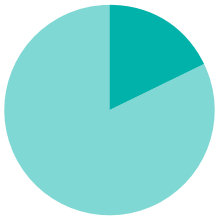
미래는 하이브리드



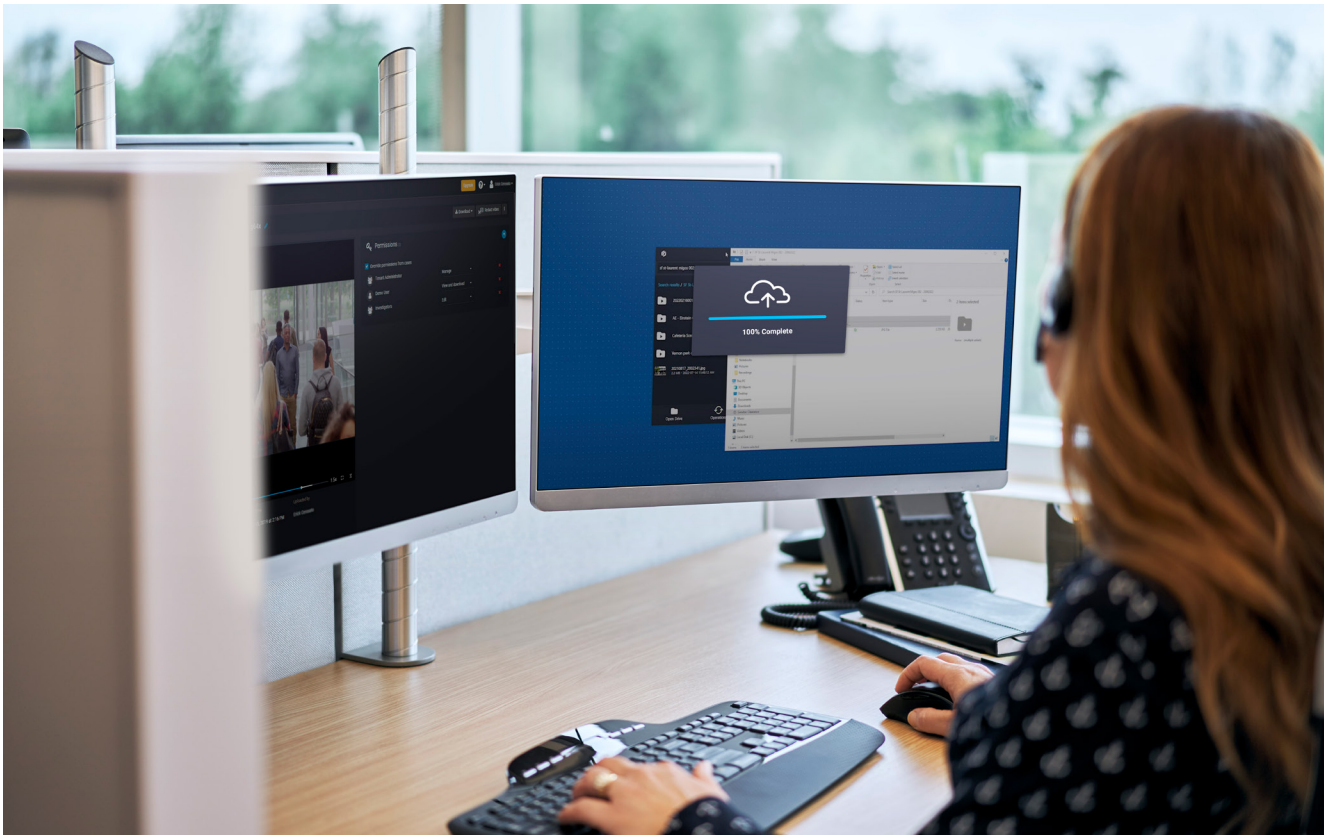
54%
온 프레미스 및 클라우드 기반 솔루션의 혼합 사용으로 이전 중이라고 답한 최종 사용자의 비율



28%
클라우드 기반 솔루션만을 이용한다고 답한 최종 사용자의 비율

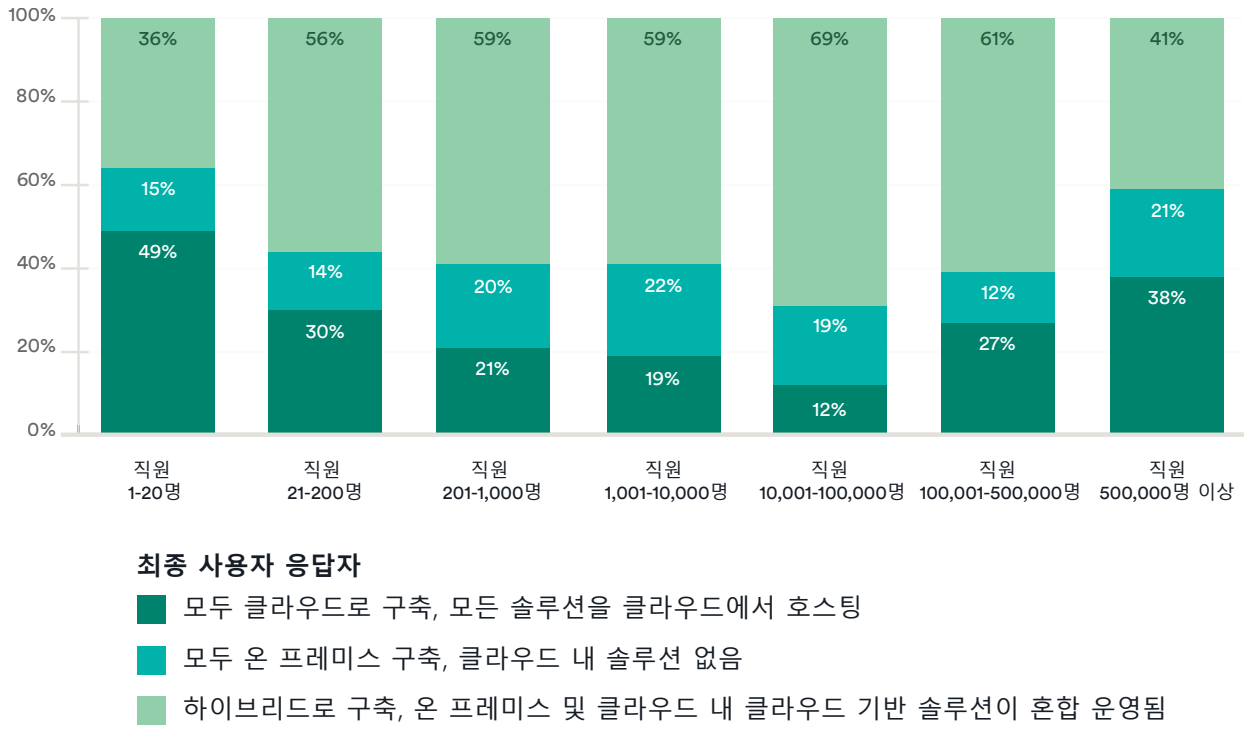


18%
클라우드 기반 솔루션을 이용하지 않는다고 답한 최종 사용자의 비율



목차로 돌아가기

향후 5년 내 클라우드 내 보안 설치와 관련한 귀사의 목표는 무엇입니까?



사이버 보안은 장애물

물리 보안 업계는 클라우드 도입 측면에서 여전히 타 업계에 뒤처져 있습니다. 해당 기술에 대한 보안 전문가들의 인식은 아직 보수적입니다. 클라우드의 사이버 보안 위험성 인식은 클라우드 도입을 지연시키는 가장 큰 이유로 꼽혔습니다. 이는 자기 충족적 장애로 볼 수 있으며, 클라우드 기반 솔루션에 내재된 사이버 보안에 대한 이해 부족에서 기인합니다.

의료 부문에서는 최종 사용자 응답자의 **26%**가 그 어떤 솔루션도 클라우드에서 호스팅하지 않을 것이라고 답했으며, 국가/지방 정부 부문에서는 **24%**가 같은 답을 선택했습니다. 이들 부문이 사무 생산성 도구를 클라우드에 설치할 준비를 하고 있는 한편, 물리 보안 업무를 클라우드로 이전하는 것에 대한 저항도 잔존하는 것으로 보입니다.

> “[물리 보안에서] [클라우드] 기술을 활용하는 문화의 부족”
>
> – 최종 사용자 설문 응답자

목차로 돌아가기

제네텍의 시각

사이버 보안이 클라우드 도입에 있어서
장애물 역할만 하는 것은 아닙니다. 위기 관리를 위한
제어 장치와 협력업체, 절차 및 매커니즘을 마련하면
됩니다. 올바른 선택을 하고 적절한 업체와 협력한다면
공동의 책임이 높은 보안성을 보장할 수 있습니다.

Mathieu Chevalier
제네텍 매니저 겸
수석 보안 설계자
제네텍

목차로 돌아가기

물리 보안 및 관련 데이터는 필수요소

팬데믹으로 인한 제약 속에서 물리 보안은 종종 사람들이 건물 내에서 안전하게 이동할 수 있도록 돕는 역할을 했습니다. 물리 보안은 사회적 거리두기 유지, 인원 수 집계, 마스크 착용 여부 확인 등에 도움이 될 수 있습니다. 하지만 팬데믹 제약이 대부분 사라진 현 시점에서 물리 보안은 여전히 자산과 사람을 안전하게 보화기 위한 필수적인 지출분야이기보다는 범죄에 대응하기 위한 도구로 간주됩니다. 물리 보안은 기업 업무 절차의 디지털화에서 핵심 요소로 자리잡았습니다.

63%

물리 보안 및 관련 데이터가 필수적이라고 답한 최종 사용자 응답자의 비율.
2021년 설문 결과 수치(68%)와 유사함.

특히 VMS는 풍부한 데이터를 제공합니다. 이미 VMS 시스템을 충분히 갖춘 기업도 있겠지만, 그렇다 해도 기존 데이터를 활용해 새로운 결과물 및/또는 부가가치를 창출함으로써 경영 프로세스를 근본적으로 바꿀 수 있습니다. 유통 기업의 고객 모니터링이나 신호등 점멸 간격 조절을 통한 시내 교통 체증 완화 등이 그 사례입니다.

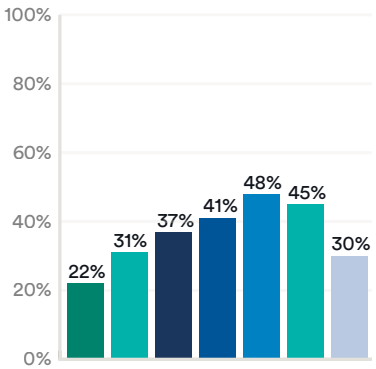
또한 기업이 성장함에 따라 물리 보안 데이터의 가치와 사용에 대한 시각도 변화하는 것으로 보입니다. 직원 수가 100,000명 이상인 기업 내 최종 사용자 응답자 중에서는 직원 수가 적은 기업에 비해 물리 보안 및 관련 데이터가 필수적이라고 답하는 비율이 높았습니다.
이는 규모가 큰 기업이 소규모 기업보다 디지털 전환 대응에 더 앞서 있기 때문일 것입니다.
물리 보안 시스템 전반에 걸쳐 수집된 데이터로부터 부가 가치를 창출해내기 위해서는 충분한 데이터 관리와 구조를 갖추는 것이 관건입니다.

최종 사용자 부문 내에서 물리 보안 및 관련 데이터가 필수적이라고답한 응답자 비율이 가장 높았고, 특히 주목할 만한 집단은 운송 부문의 최종 사용자였습니다(71%). 이 부문에서 물리 보안은 직원과 승객의 안전과 관련해 핵심적인 역할을 수행할 뿐만 아니라 운영 시간 엄수를 위한 엄격한 기준을 준수하는 데에도 도움이 됩니다.

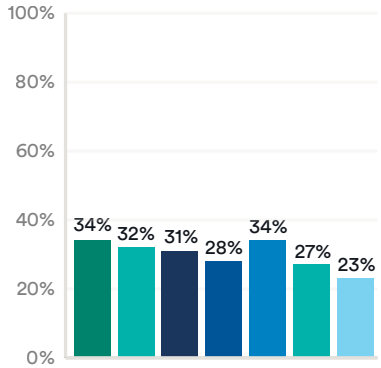
목차로 돌아가기

물리 보안이 업무에서 수행하는 중대한 역할

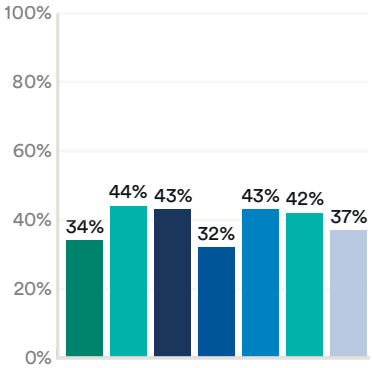
기업 규모별로 살펴본 물리 보안 및 관련 데이터에 대한 인식



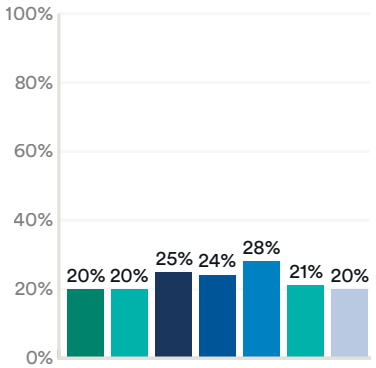
규제 지침에 대한 준수를 보장하는 방법



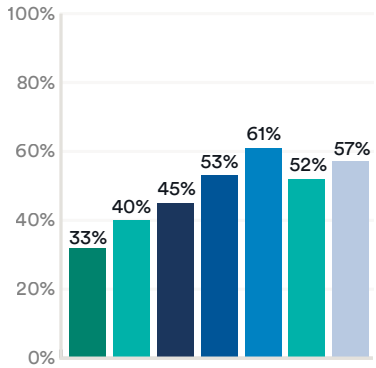
효율성 향상 및 통찰을 통해 고객 만족도를 개선하는 방법



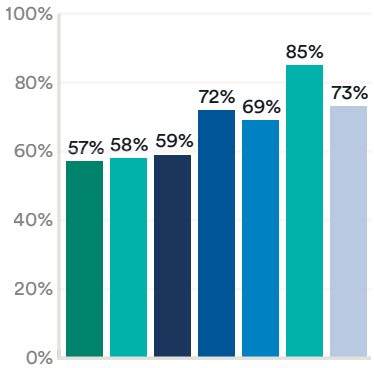
사업 생산성, 효율성, 자산 최적화를 전반적으로 개선할 수 있는 방법



운영비를 절감하는 방법



시설/사무실을 보안하는 방법



직원, 시민, 고객, 자산 보호, 지적재산의 안전성을 지원하기 위해 사업에 필수적

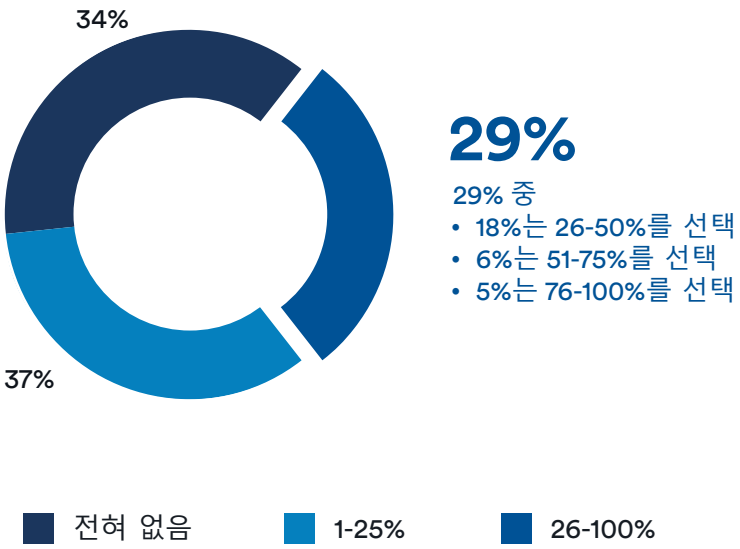
- 직원 1-20명
- 직원 21-200명
- 직원 201-1,000명
- 직원 1,001-10,000명
- 직원 10,000-100,000명
- 직원 100,001-500,000명
- 직원 500,000명 이상

목차로 돌아가기

여전히 최우선 사항인 사이버 보안

2021년 설문조사에서는 응답자의 54%가 물리 보안 운영 인력의 25% 이상이 원격으로 근무하는 기업이라고 답했습니다. 2022년 설문에서는 이 수치가 29%로 하락했습니다.

귀사의 물리 보안 운영 담당 직원 중 원격 근무에 배정된 직원의 비중은 어떻게 됩니까?



흥미롭게도 유럽 응답자의 46%와 중남미 응답자의 48%는 원격 근무를 하는 물리 보안 운영 직원이 전혀 없다고 답했습니다. 이는 미국 및 캐나다의 21%, 영국의 단 15%와 비교되는 수치입니다.

팬데믹으로 인한 제약이 완화되면서 원격 근무가 감소했습니다. 하지만 2021년 설문과 마찬가지로 응답자 전체가 직면한 직원 및 방문객 안전과 관련한 가장 큰 문제는 사이버 보안이었습니다. 전체 응답자의 49%가 올해 소속 기업에서 사이버 보안 개선 전략을 실행했다고 답한 점은 놀랍지 않은 결과입니다.

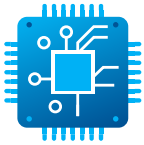
100,000명 이상의 직원을 보유한 기업에서는 이러한 경향이 더 높은 비율로 나타나 인원이 적은 기업에 비해 이들이 겪은 가장 큰 직원 및 방문객 안전 관리 문제는 사이버 보안이었음을 알 수 있었습니다. 이는 규모 있는 기업의 IT 시스템의 복잡성이 증가했다는(보호하고 관리해야 할 기기의 수 포함) 점과 이로 인해 사이버 보안 취약성이 커질 수 있다는 염려 때문일 수 있습니다. 이는 또한 규모 있는 기업이 사이버범죄자 입장에서 보다 매력적인 대상이라는 인식 때문일 수도 있습니다.

여전히 최우선 사항인 사이버 보안

사이버 보안 노력이 집중되는 분야

40%

출입통제



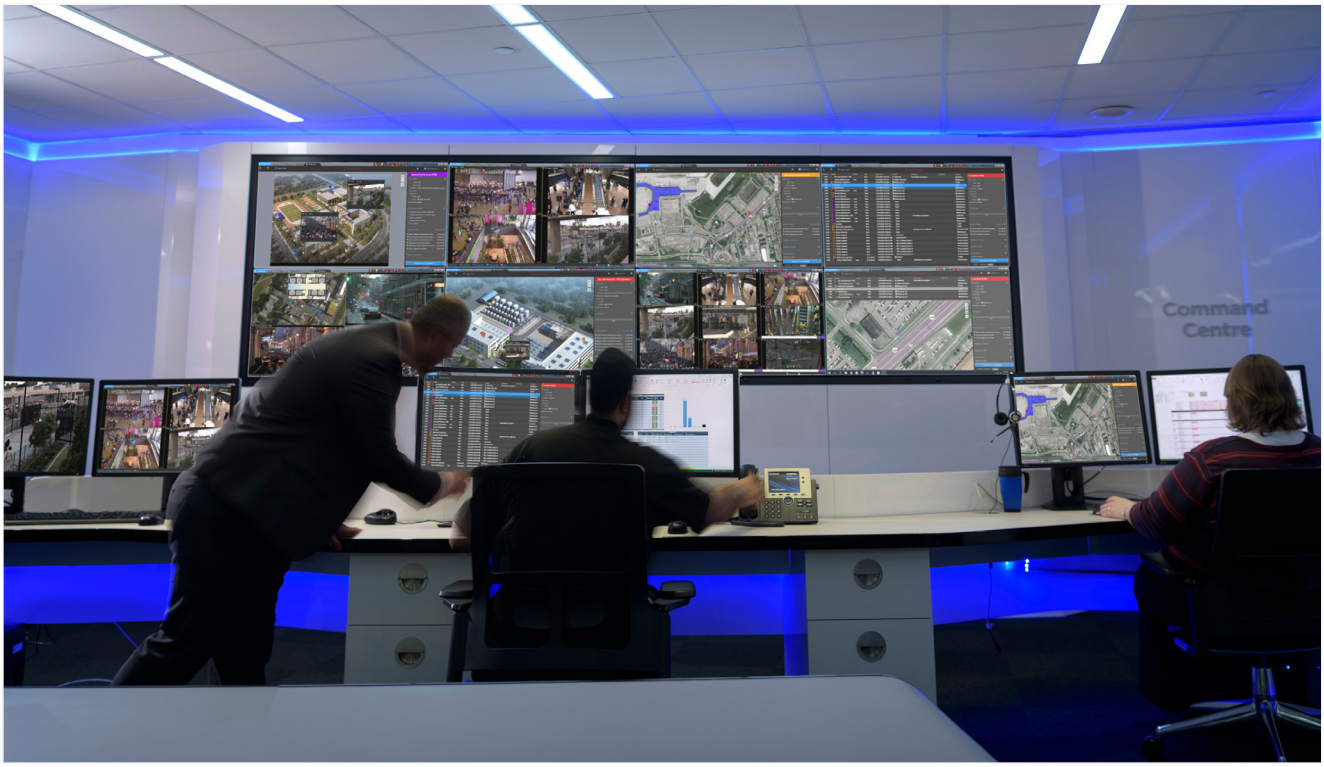
39%

보안 하드웨어 관련 사이버 강화

37%

강력한 패스워드 정책

클라우드가 사이버 보안 위험으로 인식되고 있다는 점은 물리 보안 솔루션을 위한 클라우드 도입 확대를 크게 저해하고 있습니다. 응답자들은 물리 보안 애플리케이션을 위한 클라우드 기반 솔루션 도입이 지연되는 가장 주요한 요인으로 이러한 위험성 인식을 꼽았습니다. 이와 유사하게, 최종 사용자들은 이러한 위험성 인식을 소속 기업이 보안 시스템의 클라우드 설치를 포기하게 만드는 가장 중요한 요인으로 꼽았습니다. 그럼에도 불구하고 본 보고서에서 앞서 제시한 바와 같이 클라우드로의 물리 보안 이전이 점진적으로 이어지고 있습니다.



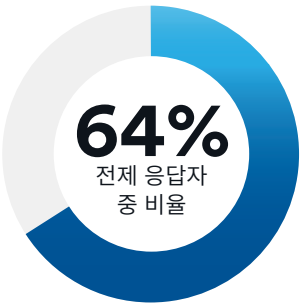
목차로 돌아가기

물리 보안의 통합

일부에게 팬데믹 관련 제약은 VMS와 출입통제 시스템을 통합하는 추가 기폭제 역할을 했습니다. 일부 최종 사용자는 이를 기회로 시설 이용자의 안전한 이동을 효과적으로 관리할 필요가 있었기 때문입니다. 이러한 방식에 대한 수요가 증가함에 따라 전문성을 높이고 통합의 이점에 대한 인식이 개선되어 최종 사용자에게 이 방식을 더 많이 추천하게 된 시스템 통합(SI)도 있을 것입니다.

설문 결과에 따르면 미국 및 캐나다 지역 최종 사용자들은 융합형 비디오 시스템 및 출입통 시스템(영상 및 출입통제 소프트웨어가 단일 제조업체가 만든 하나의 시스템으로 통합)을 설치한 사례가 가장 많았습니다.

미국 및 캐나다 응답자의 44.4%는 융합형 VMS와 출입통제 시스템을 설치했다고 답했으며, 이는 나머지 지역 전체보다 높은 수치였습니다.



물리 보안 도입에서 VMS와 출입통제를 모두 수행하고 있다고 응답

위 64% 중 75% 이상은 다음에 해당됩니다.

- 각기 다른 공급업체의 VMS와 출입통제 시스템 간의 통합
- 단일 제조업체의 융합형 VMS와 출입통제 솔루션

기술의 변화 - 기존

팬데믹의 초기 단계에서는 방문자 관리, 정부 명령 이행, 원격 기능 개선을 지원할 수 있는 다양한 보안 솔루션에 대한 관심이 급격히 높아졌습니다. 이러한 솔루션에 대한 관심은 2021년에 하락했고, 최근 설문에 의하면 2022년에는 더욱 낮아졌습니다.

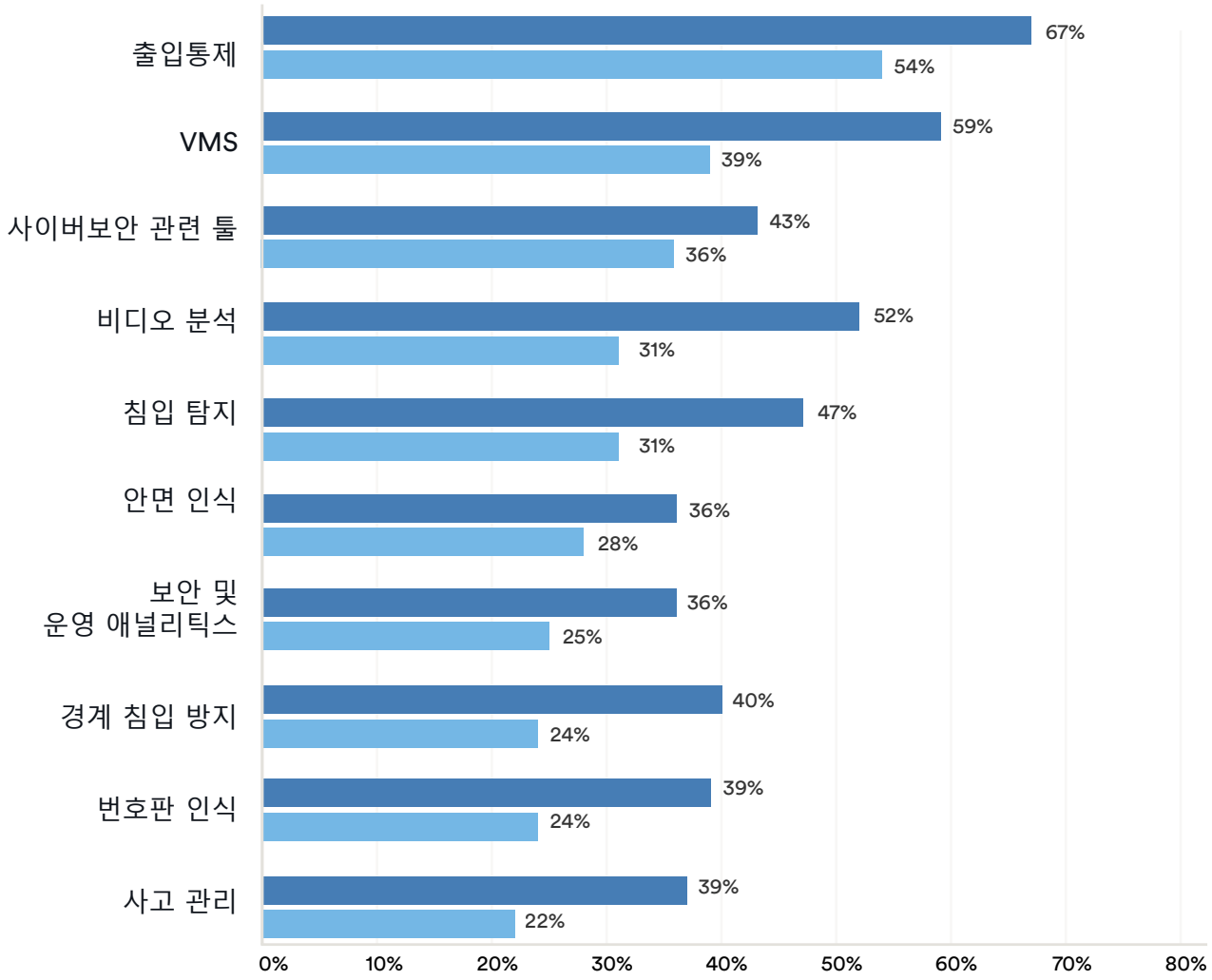
2022년 설문 응답자 전체 중 낮은 비율만이 팬데믹과 관련한 기능이 우선순위였다고 답했습니다. 2022년 설문에서는 기업들이 “기존 보안 관련” 기능에 중점을 뒀다는 사실도 드러났습니다.

기술의 변화 – 내년

앞서 본 보고서에서 언급했듯, 출입통제 및 VMS의 통합은 여러 기업에서 그 중요도가 높아졌습니다. 팬데믹 동안 핵심 시스템 뒤로 제처두었던 작업이 이제 다시 우선순위를 되찾고 있습니다. 출입통제 및 VMS는 다른 사안들과 함께 2023년 핵심 시스템 업무의 중심이 될 것입니다.

기술의 변화 - 작년 대비 내년

10대 기술 기업의 투자 계획 대상 분야



목차로 돌아가기

핵심 요점

1 경제 및 공급망은 극복가능한 난관

팬데믹 관련 제약 조치들은 2021년과 2022년 사이 대부분의 국가에서 서서히 완화되었지만 상당한 후유증을 남겼습니다. 그로 인한 경제적 여파가 제품 품귀 현상과 인력난이라는 형태로 물리 보안 업계에 영향을 미치고 있습니다. 이들 요인은 2022년에도 지속되고 있으며, 2023년 전망은 불확실해 기업들의 걱정을 계속 될 것으로 보입니다. 공급상의 변화, 경제, 경기 침체 예측과 관련한 문제가 미치는 영향에도 불구하고 설문 결과는 2023 OPEX 예산에 대해 전반적으로 긍정적인 예측이 이루어지고 있음을 보여줍니다.

2 물리 보안 시스템의 보안성 우선시

물리 보안 업계가 다른 업계에 비해 사이버 보안에 덜 집중하고 있기는 하지만, 어떤 변화가 일어나고 있으며 물리 보안 시스템 관리의 일환으로 이러한 작업을 우선시할 필요성이 대두된 것은 확실합니다. 2022년에도 직원 및 방문객 안전 관리 면에서 가장 큰 문제는 사이버 보안인 것으로 나타났습니다. 이는 2023년에도 최우선 과제가 될 것입니다.

3 계속되는 클라우드로의 이전

물리 보안 업계의 클라우드 도입이 타 산업에 비해 여전히 뒤처지고 있기는 하지만, 클라우드로 이전하는 경향이 지속될 것이라는 신호는 뚜렷합니다. 모든 신호가 하이브리드 클라우드 설치가 기업이 성공할 수 있는 방법이라는 사실을 제시하고 있습니다. 이를 통해 비용, 우려, 클라우드 이전 방식을 합리화할 수 있기 때문입니다.

31%
2023년 예산이 증가할 것으로 예상하는 응답자 비율

34%
2023년 예산이 동결될 것으로 예상하는 응답자 비율

16%
2023년 예산이 감소할 것으로 예상하는 응답자 비율

36%
향후 12개월 이내에 물리 보안 환경을 개선하기 위한 사이버 보안 관련 도구에 대한 투자를 고려 중인 응답자 비율

66%
향후 2년 내 클라우드에서 관리하거나 저장하는 물리 보안 데이터의 양을 늘릴 계획인 응답자 비율

목차로 돌아가기

제네텍의 시각

최종 사용자 중 공동 서비스 제공업체는
다음에 대응하기 위해 새로운 역량을 키워야 한다는
사실을 인지하고 있습니다.

- 기저 데이터에 관심이 있는 다른 기업 이해관계자들의
  관여도 증가
- 사이버 보안에 대한 우려 극복 및 책임감 있는
  네트워크 사용
- 기술 진보 활용에 대한 관심과 자금 조달 및
  인재 부족 등의 제약 사이의 균형

Pervez Siddiqui
제품 및 운송 본부장
제네텍

부록

부록 1 - 설문조사 방법

제네텍은 2022년 8월 24일부터 9월 21일까지 물리 보안 전문가를 대상으로 설문조사를 실시했습니다.

이번 연구의 목적은 다음과 같습니다.

- 물리 보안의 운영과 환경에 대한 관점 파악
- 제품 품귀 현상과 인력난 등의 외부 문제점에 대한 기업의 대응 방식 이해
- 2023년 전 세계의 핵심 과제 이해

제출된 자료와 데이터 정리에 대한 검토를 거쳐, 분석을 위해 3,711명의 응답자들을 표본에 포함시켰습니다.

설문조사 및 분석에 대한 세부 정보

- 설문조사 대상 모집단은 물리 보안 기술을 조달, 관리하고 관련 서비스를 제공 및 사용하는 기업에서 일하는 개인에 초점이 맞춰졌습니다. 대상 모집단은 제네택 최종 사용자와 디지털 광고를 통해 모집한 인원 및 옵트인 이메일 목록을 통해 타사로부터 직접 연락을 받은 참가자입니다.
- 온라인 설문조사를 위한 초대장은 영어, 프랑스어, 독일어, 네덜란드어, 이탈리아어, 스페인어, 일본어, 한국어로 작성되어 잠재적 참가자에게 이메일로 발송되었습니다.
- 온라인 설문조사 양식은 영어, 프랑스어, 독일어, 네덜란드어, 이탈리아어, 스페인어, 일본어, 한국어로 제공했습니다.
- 최종 분석에는 연구 대상 모집단에 속하는 개인이 빠짐없이 작성한 설문조사만 포함되었습니다.
- 설문조사 표본은 미국과 캐나다, 멕시코, 중미, 카리브해, 남미, 유럽, 중동, 아프리카, 동아시아, 남아시아, 동남아시아, 중앙아시아, 서아시아, 호주, 뉴질랜드를 포함한 모든 지역에서 실시되었습니다.
- 응답률과 설문조사 완료율은 지역과 기업 규모에 따라 다양하며, 하위 표본 집합에 표본 오차가 발생할 수 있습니다.
- 응답은 물리 보안 최종 사용자, 시스템 통합(SI)이라는 두 가지 주요 대상 모집단에서 수집되었습니다. 두 모집단 중 하나로 구분한 응답자 분류를 검증하고 잠재적 오류를 제한하기 위해 데이터 정리가 수행되었습니다. 모든 비표본 오류는 대상 모집단 외부에서 데이터를 수집함으로써 발생하는 것으로 간주됩니다 (예: 실제로 시스템 통합(SI)으로 채택되었음에도 최종 사용자로 잘못 식별되는 경우).

설문조사 계산에 대한 참고 사항:

반올림 및 설문조사 설계(등급 척도, 해당사항 모두 선택 및 다지선다형 질문 포함)로 인해 이 보고서의 모든 백분율 총계가 100%가 되지는 않습니다. 해당사항 모두를 선택하는 질문(응답자는 복수 응답 가능)에서 비율은 개별 답안을 선택한 응답자의 비율을 의미합니다.

목차로 돌아가기

부록 2 - 설문조사의 인구통계학적 정보

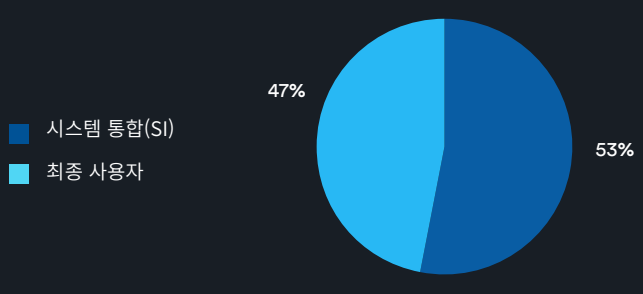
분야

보안 시스템 서비스	55%
기타	8%
교육	6%
운송	5%
은행 및 금융	3%
에너지 및 공공시설	3%
국가 안보	2%
엔지니어링 및 건설	2%
제조 및 도매	2%
기술 및 미디어	2%
헬스케어	2%
소매	2%
행정	2%
식품, 화장품, 화학약품 및 의약품	2%
운송 및 물류	1%
자산 관리	1%
전문 서비스 및 협회	1%
게임	1%

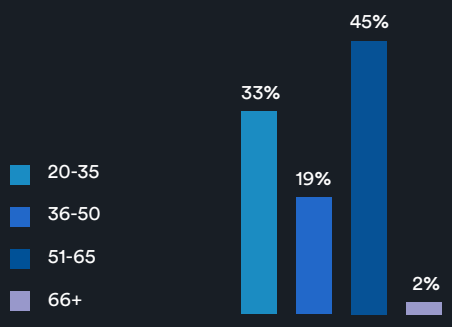
직무

엔지니어링, R&D, 시스템 설계 및 품질 보증	23%
시설/운영 관리	14%
판매	11%
정보 기술(IT)	10%
고객 서비스 또는 지원 (기술 지원 포함)	8%
프로젝트 관리 / 리스크 또는 컴플라이언스 관리	8%
행정/사무행정	6%
보안 및 안전성	5%
회계/금융	3%
행정, 법무	3%
견적	2%
마케팅	2%
법무	1%
구매 및 조달	1%
품질 관리	1%

응답자 유형

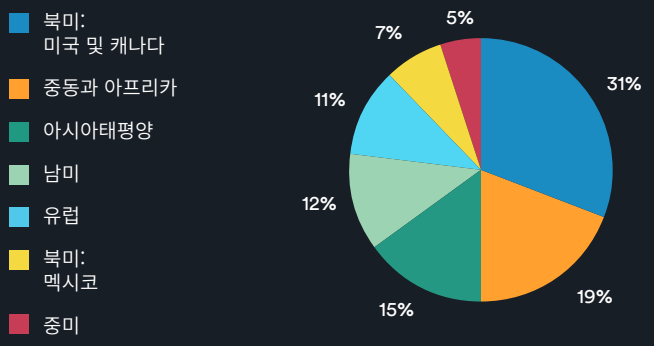


응답자의 연령



목차로 돌아가기

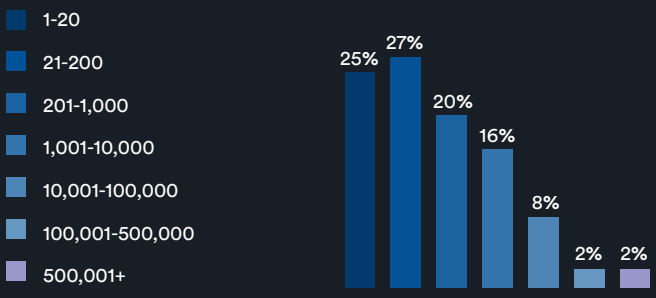
지리적 지역



기업 수익(US$)

$5M - $24.9M	31%
$25M - $199.9M	16%
$200M - $499.9M	11%
$500M - $999.9M	6%
$1B - 10B	4%
$100억+	2%
공개할 수 없음	30%

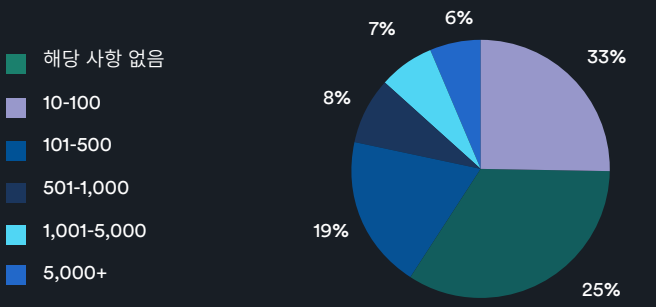
전 세계 직원 수



물리 보안 부서의 직원 수

1-20	54%
21-200	29%
201-1,000	11%
1,001-10,000	5%
10,001+	2%

VMS 도입 (카메라 수)



출입통제 도입 (카드 배지 또는 비접촉식 출입증 리더기 수)

해당 사항 없음	36%
1 - 20	13%
21 - 200	13%
201 - 1,000	14%
1,001 - 5,000	10%
5,001 +	14%

목차로 돌아가기

부록 3 - 개방형 의견

설문조사 참가자들은 일부 설문조사 질문과 관련된 추가 의견을 기입할 수 있습니다. 다음의 선정된 응답을 통해 전반적인 상황을 알 수 있습니다.

귀사에서는 다른 유형의 물리 보안 시설을 사용합니까?

- 알람
- 오디오
- 자동 방벽
- 자동 제어 주차
- 생체 인식
- 볼라드 방벽
- 차단기
- 건물 관리 시스템
- 드론
- 전기 울타리
- 긴급 경보 시스템(EAS)
- 폭발물 탐지기
- 지문 인식기
- 화재 탐지 및 진압 시스템
- 투광 조명
- 라이다
- 수하물 스캐너
- 금속 탐지기
- 이동 무선
- 레이더
- 실시간 위치추적 시스템
- RFID 자산 감시
- 보안 회전문
- 엑스레이 시스템

귀사에서 물리 보안 애플리케이션용으로 클라우드 사용을 시작한 다른 이유는 없습니까?

- 제품을 통합하고 CI 협력업체/사법부와 시스템 공유하는 능력
- 클라우드 스토리지가 더 안전하고 편리하다
- 정부 규제 준수
- 데이터 보안
- 국가 안보 지침으로부터 보안 인증 획득
- 손쉬운 사용
- NVR 도용의 위험
- 하드웨어를 도난당하는 경우 기록된 데이터 손실 방지
- 기록 중복저장/백업
- IT 직원/IT 급여 절감
- 부문 규제
- IT 인력 부족
- 작은 설비투자 규모
- 파일 접근 속도

귀사의 물리 보안 애플리케이션용 클라우드 기반 솔루션의 도입을 지연시킨 다른 요인도 있습니까?

- 충분한 대역폭 이용 가능 여부
- 클라우드에 저장된 데이터는 더 이상 나의 소유가 아니므로 자료 담당자를 통해서 사용해야 함
- 연결 문제
- GDPR
- 기술 활용 문화 부족
- 정전

귀사에서 클라우드상 보안 솔루션 설치를 포기한 다른 이유도 있습니까?

- GDPR
- 사내 데이터 센터의 공간 부족
- 중요 인프라 때문에 금지

내년에 귀하가 속한 부서에서 중점적으로 다룰 프로젝트 유형은 무엇입니까?

- 드론
- 전자식 도난방지 감시
- 화재 감지 및 진압
- IoT 자산 관리 및 추적
- 물류 재고 관리
- 비상 버튼
- 에너지 소비를 줄일 수 있는 외부 통합
- 교통 위반

목차로 돌아가기

귀사에서 2022년에 직면한 문제 중 가장 중요한 세 가지를 선택해 주세요.

- 예산상의 제약
- 정부 정책 변화
- 긴 납품 기간
- 자재 부족
- 전력 소비
- 규제
- 비용 증가

지난 해 물리 보안 부서에 영향을 끼친 인력 문제는 무엇이었습니까?

- 끊임없는 인사 이동/재배치
- 높은 물가상승률과 임금 인상
- 직원 교육을 위한 예산 부족

귀사가 올해 새롭게 가동한 프로세스나 우선과제는 무엇입니까?

- 애플리케이션 개발
- CRM/ERP 변화
- 화재 안전 시스템
- 2025년까지 탄소배출 감소
- 원격 근무

작년에 귀사에서 우선시한 기능은 무엇입니까?

- 출입통제
- 사이버 보안
- 안면 인식
- 화재 감지 및 진압
- PSIM
- 비디오 분석
- 야생동물 GPS 감시

(공급망 문제로 인해 발생한 지연 때문에) 어떤 종류의 프로젝트가 영향을 받았습니까?

- 신규 설치/프로젝트
- 사무실 이전

공급망 문제 때문에 발생한 지연 사례에는 어떻게 대응하셨습니까?

- 하청업체로부터 장비 대여
- 재고 증가
- 사전 구매

지난 한 해 동안 귀사가 최근에 실행한 사이버보안 및 데이터 보호 기능은 무엇입니까?

- 정보 시스템 감사
- ISO27K 인증
- IO 보안 기기를 위해 VLAN 분리
- 긴급 대책 운영
- 아웃바운드 소통만 운영
- VPN
- 특정 IP 주소 및 커뮤니케이션 포트에 대한 화이트리스트 작성

귀사의 고객사에서 자주 요청하는 다른 원격 기능이 있습니까?

- 출입통제 감시
- GIS 기반 지도 사용
- 활성화 및 비활성화
- 텔레그램(Telegram), 시그널(Signal) 또는 왓츠앱(Whatsapp) 등 메세지 플랫폼으로 알림 전송
- 사례 관리
- 데이터 개인정보보호
- 진단 및 시스템 건전성
- 전자 자산 보호 시스템(EAS)
- 지리위치
- 경비 순찰 감시 시스템
- 보안 시스템상 HVAC 통합 제어
- 화재 경보 시스템과의 통합
- 인터콤
- 외부로 실시간 비디오 공유
- 물류 경로 관리
- 간호사 호출
- 비상 버튼
- 예측 유지보수
- 원격 오디오 커뮤니케이션
- 원격 유지보수
- 외부 시스템 관리
- UAVS 원격 제어
- 가상화

목차로 돌아가기

귀사의 고객은 다음 12개월 동안 물리 보안 설치를 발전시키거나 개선하기 위해 어떤 솔루션에 투자하고 싶어합니까?

- 긴급 경보 시스템(EAS)
- 화재 탐지 및 진압 시스템
- 비상 버튼
- 피플 카운팅
- 라디오파를 이용하는 객체 탐지 기술을 통한 물체의 간격, 고도, 방향 및 속도 파악
- 열 감지
- 야생동물 GPS 감시

현재 공급망 문제와 관련한 하드웨어 조달 및 재고 문제를 완화하기 위해 어떠한 조치를 취하고 계십니까?

- 출시 전 고객의 사전주문 허용
- 대안이 없는 일부 프로젝트는 연기함
- 전문 서비스 및 기술 지원으로 역량 집중
- 리드타임 연장
- 쉽게 고칠 수 있는 전자기기를 재사용하기 위해 수리 센터 마련
- 시스템 재설계
- 중고 장비 활용

밀린 설치 작업에 의해 영향을 받는 다른 운영 업무가 있습니까?

- 자금 이용
- 모든 업무가 영향을 받음
- 자금 운용, 청구서 업무, 소득 징수
- 원격 근무에 대한 사이버 보안 관리
- 전자기기 및 기타 장비
- 환경 안전성
- 모든 것이 연결됨
- 인적 자원
- 물류
- 유지보수 협력업체
- 제조
- 운영
- 동원 가능한 숙련된 인력
- 솔루션 포트폴리오에 반영하려는 신규 브랜드에 대한 교육이 지연됨

제네텍 소개

제네텍은 보안, 운영 및 인텔리전스 부문을 아우르며,
광범위한 솔루션 포트폴리오를 보유한 혁신적인 테크놀로지 기업입니다.
제네텍의 주력 제품인 'Security Center'는 IP 기반 VMS, 출입통제,
자동 번호판 인식(ALPR), 커뮤니케이션 및 영상분석을 융합하는 오픈 아키텍처
플랫폼입니다. 또한 정부, 기업, 교통 및 우리가 살아가는 공동체의 보안 수준을
향상시키고 새로운 수준의 운영 인텔리전스를 제공하기 위해, 클라우드 기반
솔루션 및 서비스를 개발하고 있습니다. 제네텍은 1997년에 설립되어 캐나다 퀘벡
몬트리올에 본사를 두고 있으며, 159여 개 국가의 재판매업자, 통합업체, 공인 채널
파트너 및 컨설턴트로 구성된 방대한 네트워크를 통해
전 세계의 고객에게 서비스를 제공하고 있습니다.

제네텍에 관한 자세한 내용은
genetec.com을 확인하시기 바랍니다.

이 보고서에 대한 자세한 내용은
Genetec-research@genetec.com으로 문의하세요.

Genetec Inc.
genetec.com/ko/locations
info.kr@genetec.com
@genetec