Securitas Technology

2026 Global Technology Outlook Report

securitastechnology.com

목차

Introduction

전략적 파트너

세계 최고의 기술 제조사, 혁신가, 기술 전문가

환영 및 감사의 말

2026 글로벌 기술 전망 보고서를 소개합니다.

전 세계 Securitas Technology 임직원을 대표하여,
제8회 글로벌 기술 전망 보고서를
여러분께 소개하게 되어 매우 기쁘게 생각합니다.

먼저, Securitas Technology에 대한 지속적인 신뢰와
협력으로 올해 보고서의 방향을 제시해주신
고객 여러분께 깊은 감사를 드립니다.

또한, 전략적 파트너 및 업계 전문가 여러분의 소중한
기여에도 깊이 감사드립니다.
여러분의 전문성과 혁신에 대한 열정이 이번 보고서를
완성하는 원동력이 되었습니다.

**2025년 보고서는 고객과 업계 모두로부터
큰 호평을 받으며, Securitas Technology에게
또 하나의 이정표가 되었습니다.**

**전 세계 수많은 조직에 수만 건의 고품질 통합
보안 프로젝트를 제공하는 동시에,
지속적인 기술 혁신을 통해 새로운 기술과
서비스, 그리고 혜택을 선보였습니다.**

주요 성과는 다음과 같습니다:

1. 보안 시스템의 전력 소비 및 이에 따른 온실가스 배출량 데이터를 기록하는 혁신적인 지속가능성 이니셔티브를 시작했습니다. 이를 통해 에너지 사용에 대한 인식을 제고하고, 고객이 보다 지속가능한 보안 솔루션을 선택할 수 있도록 지원했습니다.

2. 업계 최고 수준의 보안 관리 디지털 플랫폼인 SecureStat® HQ™에 지속적으로 투자하여, 고객이 보안 프로그램을 보다 명확히 이해하고 효율적으로 관리할 수 있도록 새로운 기능과 혁신을 추가했습니다.

3. 보안산업협회(SIA)와의 협력을 통해 새로운 테크니션 견습 프로그램을 발표하며, 차세대 보안 전문가 양성에 대한 우리의 의지를 다시 한 번 보여주었습니다

2026을 맞아 새롭게 구성된 이번 전망 보고서는 시장 데이터, 전략적 기술 파트너, 업계 기술 전문가, 그리고 전 세계 Securitas 보안 전문가들의 통찰을 새롭게 담았습니다. 이번 보고서에는 최신 정보와 실질적인 인사이트가 풍부하게 수록되어 있습니다.

Securitas Technology에서, 우리는 고객과의 관계를 서비스 제공 이상의 것으로 봅니다. 신뢰할 수 있는 보안 기술 자문 파트너로서, 고객이 끊임없이 변화하는 보안 산업의 트렌드와 이슈를 선도하도록 지원합니다. 본 보고서가 SI 분야의 기술 트렌드에 초점을 맞춘 업계 주요 자료로 자리 잡은 것을 자랑스럽게 생각합니다.

이 보고서는 현재 및 미래 시장 동향을 평가하고, 새로운 위협을 예측하며, 신기술을 이해하고, 향후 조직의 보안 로드맵과 기술 투자를 자신 있게 계획하는 데 도움을 드릴 수 있도록 구성되어 있습니다.

시장 조사 기반의 데이터 인사이트, 주목해야 할 주요 기술 트렌드, 전략적 파트너의 최신 혁신, 그리고 향후 보안의 미래를 대비하기 위한 전문가의 조언까지 보고서의 각 섹션을 통해 유익한 정보를 탐색해 보시기 바랍니다.

Tony Byerly
Global President & Chief Executive Officer
Securitas Technology

Securitas Technology 소개

안전과 보안에 집중하는 글로벌 기술 파트너

Securitas Technology는 6개 대륙 전역에서 깊이 있는 혁신과 전문화된 SI 기술 역량을 바탕으로, 운영 및 서비스 품질을 보장하는 강력한 글로벌 인프라를 제공합니다.

40+ 개국 이상

보안 기술 역량 및 운영 거점 보유
전 세계 6개 대륙에서 활동

→ 6개 **대륙**

→ 글로벌 2위 **상업용 통합 보안 분야**

---

100 만 개 이상

전 세계 고객

→ 160만 개 이상의 **모니터링 연결**

→ 매년 100만 **건 이상의 유지보수, 점검 및 서비스 수행**

13,000 이상

전 세계 임직원

→ 5,000명 이상의 **기술 전문가**

→ 500명 이상의 **엔지니어, 설계자, 혁신가**

우리의 기술, 서비스, 그리고 업계 전문성에 대해 더 알아보세요 → securitastechnology.com

복잡함 속에서 단순함을 제공하는 글로벌 비즈니스 파트너

수천 가지의 SI 제품, 시스템, 그리고 서비스를 선택할 수 있는 시대에, 우리는 고객이 혼란 속에서 필요한 요구를 명확히 파악하도록 돕습니다.

기술은 그 어느 때보다 빠르게 발전하고 있습니다. 당사의 전문가는 침입 감지, 영상 보안, 출입 통제, 화재 감지, 통합 시스템 등 최신 기술 혁신을 선도하고 있어 고객이 미래 기술을 보안 로드맵에 반영하도록 지원할 수 있습니다.

맞춤형 통합 보안을 위한 신뢰할 수 있는 자문 파트너

당사는 기업들과 긴밀히 협력하며 단순한 보안 기술 공급자를 넘어, 장기적인 관점에서 고객에게 맞춤형 경험을 제공하는 신뢰받는 조언자이자 헌신적인 파트너로서 함께합니다.

세계 최고 수준의 보안 기술과 고객의 연결

세계 유수의 보안 기술 혁신 기업, 기술 전문가, 제품 제조사와의 긴밀한 파트너십을 통해, 오늘날 가장 진보적이고 지속가능한 보안 솔루션을 고객에게 제공합니다.

비즈니스 보안이 창출하는 가치

우리는 각 고객의 보안 팀과 완벽히 통합되어, 시스템 설계, 설치, 통합부터 사전 모니터링, 예방 정비, 그리고 지능형 원격 서비스까지 보안 기술의 모든 영역에서 종합적인 서비스를 제공합니다.

Securitas Technology

AI에 대한 우리의 접근 방식

함께 만들어가는 보안의 미래

이번 보고서는 수십 년간 다듬어온 보안 기술 혁신 방식의 결과물 중 하나로, 세계에서 가장 앞선 복합 보안 프로젝트들을 성공적으로 수행하며, 수많은 기업이 보안을 지속적으로 최적화하도록 지원해왔습니다.

고객 중심의 혁신 추진

무엇보다 당사의 혁신은 고객과의 긴밀한 협력과 산업별·지역별 보안에 대한 깊은 이해에서 비롯됩니다. 시큐리티 심포지엄, 고객 자문위원회, 세계 유수 제조사 및 기술 전문가들과의 협업, 그리고 업계 전반에 걸친 적극적인 참여를 통해 우리는 더 나은 기술을 탐색하고 발전시킵니다.

또한, 고객 참여 센터(Client Engagement Centers)와 기술 평가 연구소(Technology Evaluation Labs)를 통해 고객과 잠재 고객은 최신 기술을 직접 체험하고 업계를 선도하는 기술 트렌드를 파악할 수 있습니다.

글로벌 전략적 파트너십

우리는 보안 기술 혁신이 전 세계의 유수한 기업이 새로운 아이디어를 추구하고 신제품을 도입하는 생태계의 결과임을 잘 알고 있습니다. Securitas Technology는 보안 하드웨어, 소프트웨어, 분석 및 클라우드 인프라 분야의 세계적인 선도 기업들과 협력하고 있습니다.

강력한 내부 평가 프로세스

글로벌 기술 전략 및 혁신 팀 (Global Technology Strategy and Innovation Team)은 전 세계 보안 전문가들로 구성되어 있으며, 고객의 잠재적인 요구를 충족하기 위해 항상 앞을 내다봅니다.

이 팀은 비즈니스 리더 및 전략적 파트너와 협력하여 새로운 기술의 이점을 분석하고, 다양한 기술의 적절한 적용 방안을 연구합니다.

또한 신제품이 기술적으로 안정적이고 상업적으로 실행 가능한지 철저히 검증하여, 당사의 솔루션과 서비스를 지속적으로 개선하고 있습니다.

인재와 프로세스의 우수성

마지막으로, 우리는 기술과 지역을 넘나드는 전문성을 바탕으로 혁신을 고객에게 전달합니다. 통합 보안 기술의 설계, 설치, 모니터링, 유지보수, 그리고 지속적인 업데이트 역량을 갖춘 당사는 기업 규모에 상관없이 모든 조직이 신뢰하는 자문 파트너로 자리매김하고 있습니다.

Securitas Technology의 글로벌 클라이언트 프로그램은 전 세계에 걸쳐 복잡한 보안 요구를 가진 글로벌 기업에게 이러한 혜택을 맞춤형으로 제공할 수 있도록 전문성을 갖추고 있습니다.

Securitas Technology의 글로벌 클라이언트 프로그램에 대해 더 알아보세요 securitastechnology.com/global-clients-program

SecureStat® HQ™ 보안 관리 플랫폼

보안 운영에 대한 명확성과 제어력을 확보하여 지속적인 개선을 실현하세요

SecureStat® HQ™는 보안 관리를 단순화하고, 사용자를 보안 시스템과 Securitas Technology의 서비스에 연결하며, 데이터를 기반으로 보안 및 비즈니스 성과를 최적화하는 올인원 디지털 보안 관리 플랫폼입니다.

엔터프라이즈급 사이트 제어

- 회사 전체의 여러 사이트를 한눈에 관리하고 볼 수 있습니다.
- 사이트 일정(Site Schedule)을 설정하여 일관성을 유지할 수 있습니다.
- 연락처 및 호출 목록을 편집하여 최신 정보를 유지합니다.

클라이언트 게이트웨이와 연동

- 서비스 티켓을 생성하고 지원팀과 직접 연결할 수 있습니다.
- 인보이스(청구서)를 조회하고 결제할 수 있습니다.
- 실시간 및 녹화된 영상을 확인할 수 있습니다.

효율적인 시스템 관리

- 출입 통제, 영상 보안, 화재, 침입 감지 등 여러 보안 스템을 통합적으로 제어할 수 있습니다.
- 여러 시스템에 걸친 사용자 접근 권한을 관리합니다.
- 인터넷 연결만으로 어디서든 시스템 테스트를 수행할 수 있습니다.

지능형 데이터 인사이트

- 동적이고 맞춤화된 보고서를 제공합니다.
- 예외 상황 및 이벤트 보고 기능을 제공합니다.
- 보고서 구독 기능을 통해 표준화된 리포트를 자동으로 제공합니다.

실시간 이벤트 관리

- 활동 메신저를 통해 여러 지점의 활동을 시간으로 확인합니다.
- 경보 메신저를 통해 알람을 확인하고 즉시 대응합니다.
- 서비스 메신저를 통해 서비스 요청 상태를 업데이트합니다.
- 설치 프로젝트 진행 상황을 모니터링합니다 (곧 출시 예정).

유연한 구독 플랜 선택

- Basic, Advanced, Premium 등 다양한 플랜이 공됩니다.
- 각 조직의 필요에 맞게 맞춤형 구성 가능합니다.
- SecureStat 360® 라이프사이클 관리 서비스 등 SecureStat® HQ™를 통해 제공되는 고급 서비스를 이용할 수 있습니다.

보안 성능과 기술을 최적화하기 위한 SecureStat® HQ™ 기능

SecureStat 360® 보안 기술 라이프사이클 관리

보안 자산의 효과적인 라이프사이클 관리를 통해 보안성과 조직 가치를 극대화합니다.

장비 수명 극대화:

장비의 설치 시점, 서비스 이력, 교체 권장 시기를 명확히 파악할 수 있습니다.

비용 효율적인 업그레이드 계획:

교체가 필요한 장비를 한눈에 확인하여 효율적인 업그레이드 계획을 수립하고, 데이터를 기반으로 투자 결정을 내릴 수 있습니다.

알려진 취약점에 대한 노출 최소화:

소프트웨어 및 펌웨어 버전과 사용 종료(EOL) 상태를 쉽게 모니터링하여, 구식 펌웨어나 단종 예정 장비를 사전에 관리할 수 있습니다.

CO2e 배출량 문서화:

장비별 전력 소비로 인한 CO2e(이산화탄소 환산 배출량)를 확인하고, 지속가능성 목표에 맞춰 보안 투자를 결정할 수 있으며 관리할 수 있습니다.

SecureStat® Video

이벤트와 관련된 실시간 및 녹화 영상을 확인할 수 있습니다.

SecureStat® Access

출입 통제 시스템을 원격으로 관리할 수 있습니다.

SecureStat® Alarm

침입 감지 시스템을 원격으로 관리할 수 있습니다.

1 요약 보고서

2026년 보안 산업의 새로운 지평
2026년과 그 이후 보안 전문가들이 직면할 핵심 트렌드, 과제, 그리고 기회.

보고서 소개

보안 전문가를 위해 보안 전문가들이 직접 제작한 2026 글로벌 기술 전망 보고서는 다양한 독점 데이터 소스와 깊이 있는 업계 전문성을 결합하여, 상업 보안 시장의 현재와 미래를 형성하는 기술, 전략, 혁신에 대한 실질적인 인사이트를 제공합니다.

이 보고서를 구성하는 데이터와 전문성의 주요 출처는 다음과 같습니다.

시장 조사 :

Securitas Technology가 의뢰한 외부 시장 조사로, 미국, 프랑스, 영국, 독일, 스웨덴, 호주 등 6개국의 검증된 보안 전문가 575명의 응답을 바탕으로 진행되었습니다. 이 조사는 SI 기술 투자에 직접 관여하는 의사결정자 및 전문가를 대상으로, 현재의 기술 활용 현황, 향후 도입 계획, 투자 의향 등에 초점을 맞췄습니다.

2024년 고객 설문 및 자문위원회 피드백:

Securitas Technology가 주관한 설문 과정으로, 17개국 4,500명 이상의 고객이 응답했습니다. 2024 글로벌 고객 설문에는 향후 보안 기술 도입 및 투자 계획에 관한 질문이 포함되었으며, 또한 Securitas Technology 고객 자문위원회(Client Advisory Board) 구성원들의 피드백도 반영되었습니다.

이 위원회는 다양한 산업 분야를 대표하는 고객들로 구성되어 있으며, 보안 기술과 관련된 도전 과제 및 요구 사항에 대한 의견을 제공합니다.

기술 파트너 자문 과정:

Securitas Technology가 주관한 협의 프로세스로, 24개 전략적 기술 파트너로부터 설문 데이터와 업계 인사이트를 수집했습니다. 참여 파트너에는 업계 최고의 보안 제품 제조사, 개발자, 혁신가, 기술 전문가들이 포함됩니다.

내부 보안 전문가 의견:

전 세계 Securitas Technology 내부 기술 리더 및 보안 전문가들과의 인터뷰 및 연구를 통해 인사이트를 수집했습니다. 여기에는 Securitas Technology 전략 및 혁신팀 (Global Technology Strategy & Innovation Team), 글로벌 기술 검토 위원회(GTRC), 글로벌 기술 혁신 위원회(GTIC) 멤버들이 포함되었습니다.

2026 전망: 보안 전문가들이 주목하는 변화

2025년 보고서는 SI(Security Integration) 분야에서 데이터의 중요성이 점점 커지고 있음을 강조하며, 데이터가 산업 전반에 가져오는 변화—새로운 가치 창출과 더불어 클라우드 기술, AI, 데이터 분석(Data Analytics), 개인정보 보호(Data Privacy), 사이버 위생(Cyber Hygiene)과 같은 새로운 전문성을 요구하는 양상을 조명했습니다.

이러한 트렌드는 지난 1년간 더욱 가속화되었습니다. 전 세계적으로 AI 모델 개발과 일상 속 AI 활용이 폭발적으로 증가하면서, 데이터 연결성 및 데이터 센터 인프라 개선을 위한 투자가 급격히 확대되고 있습니다.

보안 기술 분야에서는 이미 수년 전부터 클라우드 인프라, 데이터 분석 및 인공지능을 활용해 왔습니다. 그러나 이제는 보안 제조사와 개발자들이 이러한 기술들의 단순한 적용을 넘어 영상 보안, 침입 감지, 출입 통제 등 다양한 영역에서 솔루션의 기능을 더욱 고도화하고 있습니다.

2026년의 보안 전망은 이미 산업 전반에 변혁을 일으키고 있는 세 가지 핵심 기술 트렌드 — **AI, 클라우드 애플리케이션**, 그리고 **고급 센서 기술 의** 지속적인 확산을 예상합니다.

이 기술의 정교함과 접근성이 높아지면서 도입률이 증가하고 있으며, 보안 장비 및 애플리케이션을 통해 수집된 데이터를 **다른 영역의 가치 창출에 적극 활용하는 방향**으로 발전할 것입니다.

이번 보고서의 조사 결과에 따르면, **직원 안전 강화가 조직의 향후 보안 투자에서 가장 중요한 요인으로 꼽혔습니다.** 또한, 2026년 보안 전문가들이 중점적으로 대응해야 할 여러 비즈니스 과제들도 다음과 같이 제시됩니다:

- **불안정한 비즈니스 환경에서 사람의 안전을 지키기**
- **실시간 대응 및 예방적 사건 관리 전략으로의 전환**
- **보안 도입을 통한 조직적 가치와 영향력 확대**

이러한 트렌드와 빠르게 변화하는 기술, 그리고 위협 환경은 조직이 보안 프로그램 내 지속적인 기술 평가 체계를 구축할 것을 요구합니다. 새로운 기술을 단계적으로 도입하고, 경험이 풍부한 파트너의 지원을 받는 접근 방식은 보안 전문가들이 새로운 기술을 원활히 통합할 수 있도록 계획하는 데 큰 도움이 됩니다.

확실한 것은, 정체는 선택지가 아니라는 점입니다. 지금 선제적으로 계획하는 것이 미래에 뒤처지지 않기 위한 최고의 보험입니다.

핵심 시사점

1

AI분야는 **생성형 AI(GenAI)** 활용 사례의 발전 (예: 자연어 검색)과 처리 능력 향상에 따라 한층 더 진화할 것입니다.

AI는 서로 다른 시스템에서 수집된 데이터통합하여, 복합적인 보안 및 비즈니스 인텔리전스를 생성하는 시스템 통합 방식의 혁신을 이끌 것입니다.

더 알아보기: 섹션 2, 페이지 22

2

클라우드 기반 기술은 이제 새로운 표준 (New Normal)로 자리 잡았으며, 앞으로 많은 보안 시스템 구현의 기반이 될 것입니다.

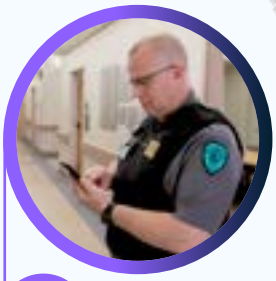
온프레미스(사내) 인프라에서 **클라우드 구성으로의 전환**은 계속될 것이며, 하이브리드 방식을 통해 중앙 집중형 관리 및 향상된 확장성과 같은 이점을 추구할 것입니다.

더 알아보기: 섹션 2, 페이지 26

3

고급 센서(Advanced Sensors)의 통합은 보안 시스템과의 호환성이 높아짐에 따라 더욱 확대될 것입니다. 조직은 센서로부터 수집되는 더 많은 데이터를 활용하여 규정 준수, 운영 효율성 향상, 그리고 고객 및 직원 경험 개선을 추구할 것입니다.

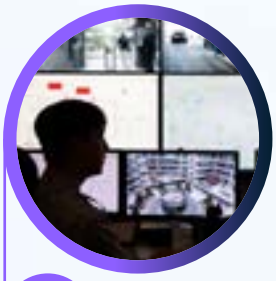
더 알아보기: 섹션 2, 페이지 30



4

높아지는 글로벌 긴장과 불안정성은 전 세계 조직에 큰 우려를 주고 있습니다. 이에 따라 직원 안전 강화와 위기 대응 커뮤니케이션을 지원하는 기술들이 우선순위로 다뤄지고 있으며, 이와 함께 리스크 인텔리전스 향상, 비상사태 대비, 재난 복구 전략 등도 강화되고 있습니다.

더 알아보기: 섹션 3, 페이지 36



5

사후 대응 중심의 사건 대응 방식은 점점 예방적 위협 감지(Proactive Threat Detection) 중심으로 전환되고 있습니다. 여러 데이터 소스와 AI 가상 에이전트가 통합된 알람 관리 도구의 사용은 자동화와 정확성을 향상시켜, 보안 요원이 더 효율적으로 업무를 수행하고 잠재적 위협을 미리 예측할 수 있도록 돕습니다.

더 알아보기: 섹션 4, 페이지 54

6

조직은 이제 보안 기술을 가치 창출(Value Driver)의 도구로 인식하고 있습니다. 보안 기술은 직원 및 고객 경험을 향상시키고, 지속가능성 목표 달성에도 기여하며, 효율성을 높이고 다양한 방식으로 비즈니스 운영을 최적화하는 핵심 도구로 자리 잡고 있습니다.

더 알아보기: 섹션 5, 페이지 72

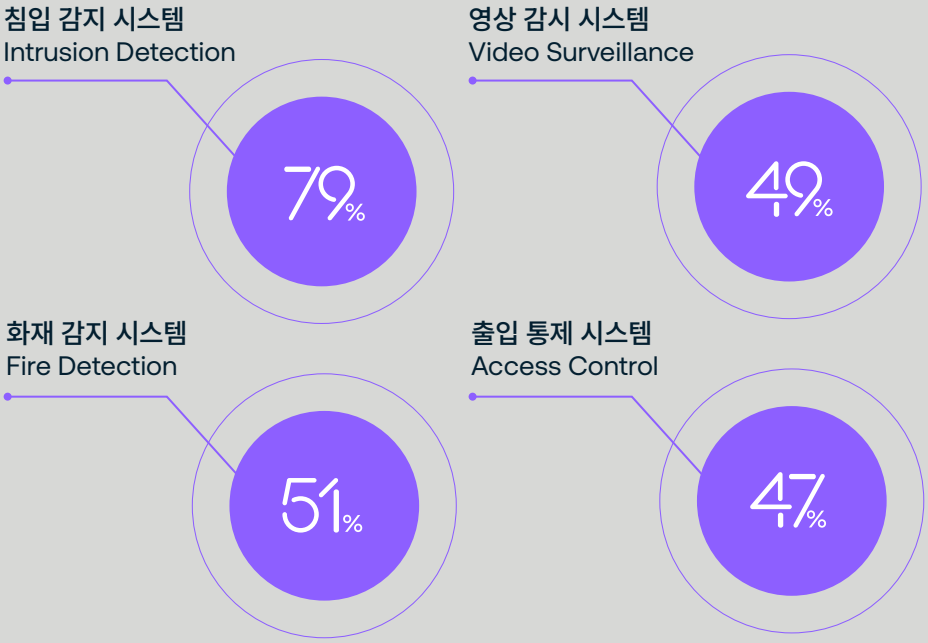
데이터 트렌드 및 인사이트

고객 동향

Securitas Technology는 2024년 12월, 고객을 대상으로
현재 사용 중인 기술과 향후 기술 도입 계획에 대한 설문조사를 진행했습니다.

가장 많이 도입된 기술[1]

현재 사용 중이라고 응답한 비율:



[1]이 조사는 Securitas Technology가 자체 브랜드로 실시한 설문으로, 총 4,540명의 고객이 참여했습니다.
참여 국가는 호주, 벨기에, 캐나다, 덴마크, 핀란드, 프랑스, 독일, 아일랜드, 멕시코, 네덜란드, 노르웨이, 스페인, 스웨덴, 스위스, 터키, 영국, 미국 등 17개국입니다.
조사는 2024년 11월에 진행되었습니다.

주요 트렌드 기술[1]

	현재 사용 중:	향후 12~18개월 내 도입 예정:
1	29% Mobile Smartphone Credentials	30% Artificial Intelligence
2	28% Cloud-Based Solutions & Storage	27% Mobile Smartphone Credentials
3	26% Visitor Management	25% Visitor Management
4	11% Artificial Intelligence	24% Predictive Analytics
5	8% Touchless Biometrics	20% Touchless Biometrics
6	7% Predictive Analytics	**20%** Cloud-Based Solutions & Storage

구독 기반 주요 기술[1]

	현재 사용 중:	향후 12~18개월 내 도입 예정:
1	**43%** Managed & Hosted Access Control	**27%** Video Alarm Verification
2	**43%** Fire & Emergency Preparedness Training	**20%** Managed & Hosted Video
3	**39%** Managed & Hosted Video	**16%** Online Client Management Portals
4	**37%** Mobile Response Guarding	**15%** Fire & Emergency Preparedness Training
5	**25%** Video Alarm Verification	**15%** Managed & Hosted Access Control
6	**24%** Online Client Management Portals	**11%** Mobile Response Guarding

데이터 트렌드 및 인사이트

시장 동향

Securitas Technology는 여러 시장의 보안 및 손실 예방 전문가를 대상으로

심층 설문조사를 실시하여 보안 기술의 핵심 트렌드와 주요 활용 사례를 파악했습니다.

클라우드 기술 도입 현황 및 계획[2]

클라우드 기반 시스템은 이제 보안 기술의 주류(Mainstream)로 자리 잡았습니다.

클라우드 도입 증가 추세

조직 내 클라우드 기반 SI 기술 활용 현황:

18%
현재 완전히 클라우드 기반 시스템을 사용 중

34%
향후 5년 내 완전한 클라우드 전환을 예상

클라우드 도입을 이끄는 효율성 요인

클라우드 기반 시스템을 도입하는 주요 이유

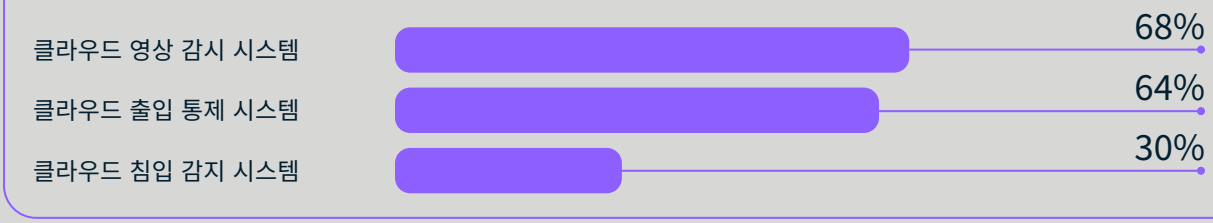
#1 – **중앙 집중형 보안 관리**

#2 – **운영 효율성 향상**

#3 – **사용 및 관리 용이성**

주요 클라우드 기반 시스템

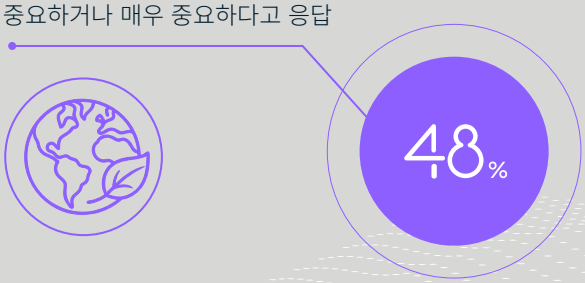
클라우드 솔루션을 사용하는 조직이 도입한 주요 시스템:



지속가능성 참여도[2]

지속가능성 관련 활동에 직접 참여

기술 선택 시 지속가능성을 중요하거나 매우 중요하다고 응답



AI 도입 현황 및 계획[2]

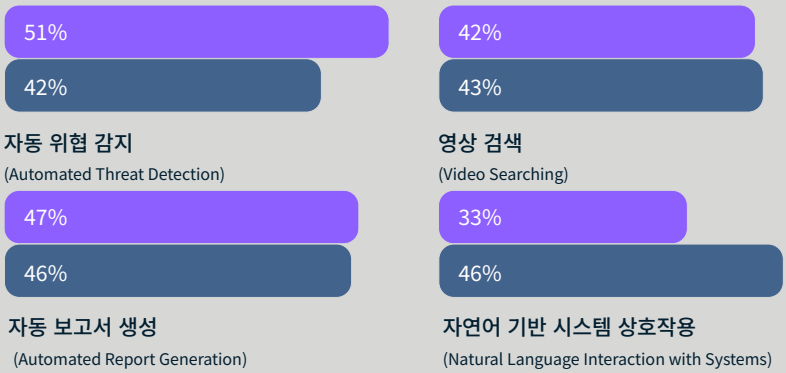
AI는 보안 기술의 핵심 요소로 자리 잡았으며, 새로운 활용 사례에 대한 관심이 높은 것으로 나타났습니다.

현재 주요 AI 활용 사례

- 36% **객체 인식** (Object Recognition)
- 35% **침입 및 배회 감지** (Intrusion and Loitering Detection)
- 27% **인원 수 계산** (People Counting)
- 26% **이상 징후 감지** (Anomaly Detection)
- 24% **차량 감지, 속도 및 방향 분석** (Vehicle Detection, Speed, and Direction)

향후 생성형 AI(GenAI) 주요 활용 관심 분야

- "매우 관심 있음" 또는
- "어느 정도 관심 있음":



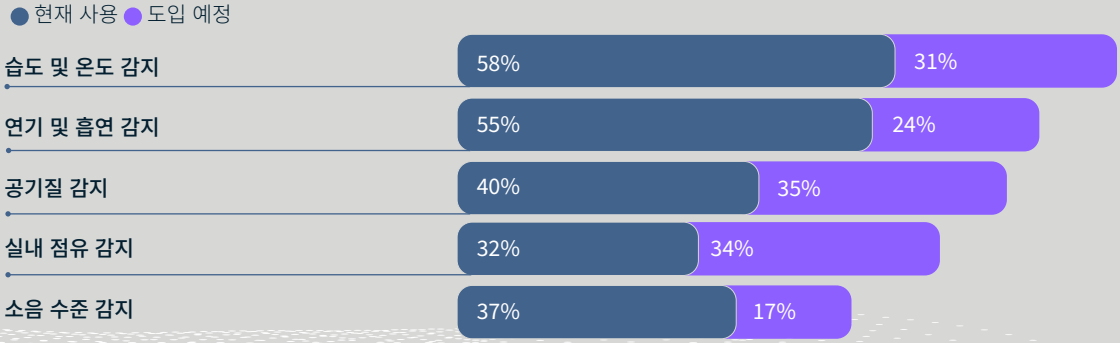
고급 센서 기술 도입 현황 및 계획[2]

고급 센서는 이미 보안의 필수 구성 요소로 활용되고 있으며, 대부분의 조직이 향후 도입 확대를 계획하고 있습니다.

보안 내 고급 센서 사용 현황

- 9% 광범위하게 사용 중
- 39% 부분적으로 사용 중
- 35% 도입 계획 중
- 16% 사용하지 않음

주요 고급 센서 활용 사례



[2]2025년 2~3월에 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 및 손실 예방 전문가 575명을 대상으로 실시한 제3자 블라인드 설문조사 결과.

파트너 인사이트

Securitas Technology는 전략적 기술 파트너들을 대상으로 보안 기술의 발전 방향과 혁신 계획에 대한 인사이트를 조사했습니다.

50%
Ranked AI as the top trend in the industry

상위 3대 보안 기술 트렌드

1 인공지능(AI) 응용 분야

"CSO부터 CEO에 이르기까지 모든 리더가, 이미 보유한 카메라를 활용해 조직이 AI를 어떻게 적용할 수 있을지 모색하고 있습니다."

Hanwha Vision

"Agentics: 문맥을 이해하고, 스스로 판단하며, 독립적으로 행동할 수 있는 자율형 AI에이전트 시스템입니다."

milestone

2 클라우드 기술

"생성형 AI 모델을 활용해 녹화된 영상을 검색할 수 있도록 지원하는 클라우드 솔루션에 대한 관심이 급격히 증가하고 있습니다."'

VERINT

"중소기업(SMB)과 분산형 기업(Distributed Enterprises)이 이러한 기술을 가장 빠르게 도입할 것으로 예상됩니다."

MOTOROLA SOLUTIONS

3 시스템 통합

"보안 시스템을 현대화하는 것은 중앙 집중화의 가치를 높여주며, 여러 구성 요소를 하나의 플랫폼으로 통합할 수 있게 합니다."

brivo
simply better security

"새로운 통합 솔루션은 중앙 관제 트웨어 배포를 단순화하여, 타 사이트 VMS(Video Management System) 설치를 더욱 용이하게 만듭니다."

EAGLE EYE NETWORKS

지속가능성 지원 단계

1 제품 설계

"지속가능성은 제품 설계의 핵심 원칙으로, 장기적인 내구성과 효율성, 재활용성을 보장하며 전력 소모와 탄소 배출을 줄입니다."

resideo

"우리의 개발 툴킷은 원자재, 수자원, 신규 자재 사용, 사용 수명 종료 후 재활용성, 재사용 가능성, 사용 중 에너지 소비, 탄소 발자국, 재정 비용 등 8가지 영역에 중점을 두고 있습니다."

ASSA ABLOY
Opening Solutions

2 장비 전력 소비

"에너지 효율적인 영상 보안 시스템을 개발하여 전력 소비와 탄소 배출을 줄이고 있습니다."

MARCH networks
A Delta Group Company

"하이브리드 및 클라우드 기반 아키텍처 지원은 조직이 하드웨어 사용량을 최적화하고 에너지 소비를 줄이며 효율적으로 확장할 수 있도록 돕는 핵심 요소입니다."

INTELLICENE
UNIFYING SECURITY. ENABLING ACTION

3 운영 관행

"제조 과정에서 물 사용을 최소화하고, 안전하다고 분류된 소재만을 선택해 유해 물질을 제거하는 목표를 세웠습니다."

AXIS COMMUNICATIONS

"IDIS 아메리카는 내구성 높은 보안 제품을 개발하여 폐기물 최소화 및 교체 주기 감소에 기여하고 있습니다."

IDIS One Solution. One Company.

제품 개발의 주요 우선순위

1

인공지능(AI) 및 분석 통합

“AI 기반 분석을 통해 실시간 사고 감지, 이상 징후 인식, 그리고 예방적 위협 대응(Proactive Threat Mitigation)을 실시합니다.”

MARCH networks
A Delta Group Company

“AI를 활용해 사용자 경험을 개선하고 운영의 속도와 확장성을 높입니다.”

VIAKOO

2

클라우드 솔루션

“확장성, 유연성, 원격 관리가 가능한 클라우드 기반 솔루션을 제공합니다.”

MOTOROLA SOLUTIONS

“엔터프라이즈급 클라우드 및 모빌리티 솔루션을 제공합니다.”

Honeywell

3

통합 및 상호운용성

“보안 시스템의 현대화는 중앙 집중화의 가치를 실현하며, 다양한 구성 요소를 하나의 플랫폼으로 통합할 수 있도록 합니다.”

“DMP 생태계 내 더 많은 개방형 API를 통해 이기종 시스템 간 호환성을 향상시킵니다.”

DMP

4

사용자 경험 및 인터페이스 개선

“이벤트 데이터를 시각화하고 분석을 단순화하여 이상 징후를 식별하고, 트렌드나 패턴을 파악하며, 이벤트 간의 연관성을 이해할 수 있도록 합니다.”

OpenEye

“모듈형, 목적 중심, 모바일 친화적인 애플리케이션을 개발하여 고객의 문제를 해결합니다.”

AMAG TECHNOLOGY
An Allied Universal Company

5

지속가능성 및 효율성

“에너지 효율적이고 환경 친화적인 솔루션에 중점을 두고 있습니다.”

SONITROL

“생산지 인근에서 원자재와 부품을 조달함으로써 탄소 배출 감소 목표를 달성하고 있습니다.”

ASSA ABLOY
Opening Solutions

> “이러한 인사이트는 글로벌 보안 혁신의 최전선에서 활동하는 당사의 전략적 파트너들이 직접 제공한 것으로, 고객에게 향후 보안 기술 개발 방향에 대한 명확한 관점을 제공합니다.”
>
> Doug Walsh | Global VP, Technology Strategy
> Securitas Technology

2

2026년에 주목해야 할 기술 트렌드

AI, 클라우드 컴퓨팅, 그리고 고급 센서 기술 분야의 혁신 속도가 가속화되면서, 보안 기술 자체뿐만 아니라 기술의 배포, 유지보수, 활용 전략에도 큰 변화를 가져오고 있습니다.

전 세계적으로 이러한 혁신적인 기술의 접근성이 높아지면서 우리의 삶과 업무 방식, 그리고 미래로 나아가는 방식이 근본적으로 변화하고 있습니다.

보안 산업에 있어 이러한 변화는 거대한 기회를 의미합니다.

세계적인 제조업체, 소프트웨어 개발사, 그리고 혁신 기업들은 영상 감시, 침입 감지, 출입 통제 등 다양한 보안 분야에서 이러한 기술을 활용해 더욱 향상된 기능을 만들어가고 있습니다. 보안 전문가들에게 이는 통합 수준의 향상, 보호 능력의 강화, 그리고 더욱 효율적인 보안 관리를 의미합니다.

인공지능(AI) 가속화

AI는 오늘날 전 세계적으로 폭넓게 사용되고 있으며, 그 혁신적인 잠재력은 여전히 글로벌 기술 산업을 주도하고 있습니다.

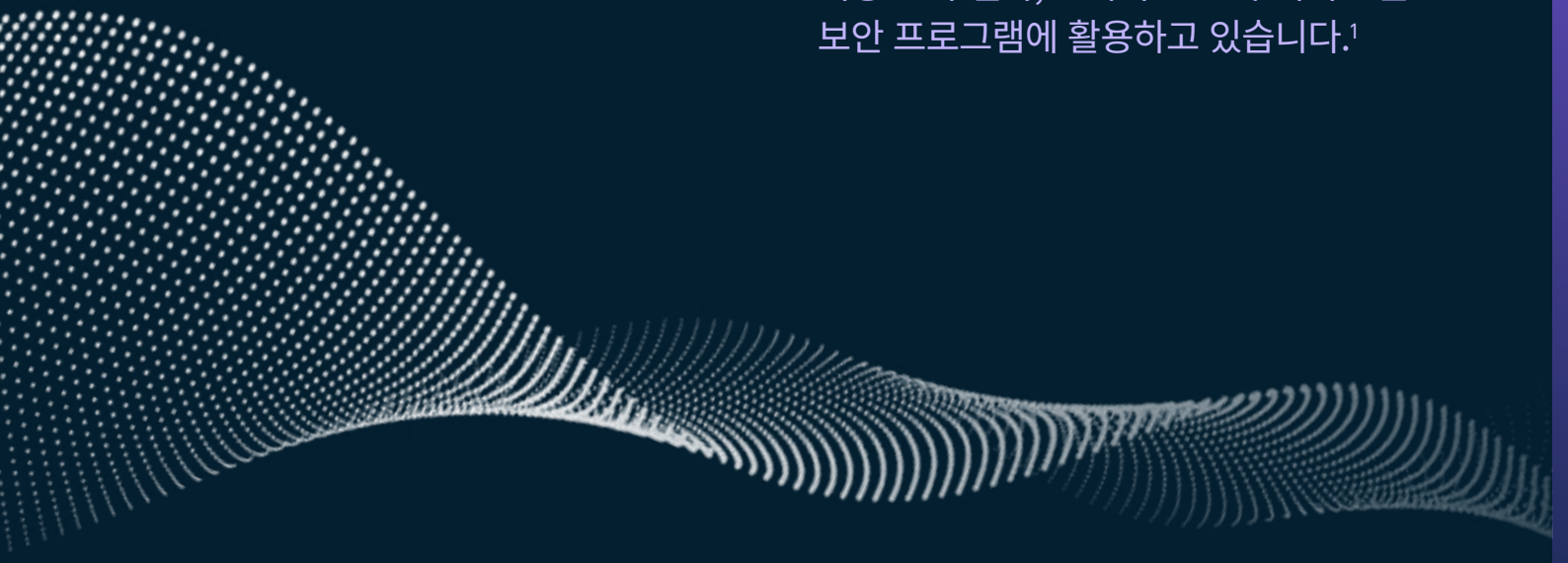
AI의 막대한 잠재력을 실현하기 위한 대규모 투자가 이어지면서, 과거에는 상상할 수 없었던 기능들이 빠르게 개발되고 있습니다.

이는 단순히 뉴스의 주제가 되는 것을 넘어, 거의 모든 산업과 사회 분야에 영향을 미치고 있습니다.

보안 기술에서도 AI는 새로운 개념이 아닙니다. 이미 머신러닝(ML)과 데이터 분석을 활용한 영상 감시 및 위협 감지, 차량 번호판 인식, 공간 점유 관리, 얼굴 인식, 객체 감지 및 추적 등 다양한 분야에서 AI가 적용되어 왔습니다.

이러한 AI 응용 기술들은 앞으로 더욱 정교해지고 확장될 것입니다. 시장 조사에 따르면, AI는 이제 보안 산업의 핵심 기술로 인식되고 있습니다.

시장 조사 결과, 조직의 70%가 이미 AI를 보안 프로그램에 활용하고 있습니다.[1]



> AI와 AI 기반 에이전트는 출입 통제, 신원 관리, 보안 관리 플랫폼 분야에서 효율성을 향상시키고 데이터 기반 의사결정을 가능하게 함으로써 보안 산업을 변화시키고 있습니다.
>
> HID

새로운 세대의 인공지능(AI)이 등장하다

2026년을 맞이하며, 인공지능(AI)은 이제 머신러닝(ML) 단계를 넘어 더 높은 수준의 자동화와 인사이트 생성을 가능하게 하고 있습니다. 바로 여기서 생성형 인공지능(Generative AI, GenAI)이 중요한 역할을 합니다.

시장 조사 결과에 따르면, 대부분의 조직이 생성형 AI의 활용 사례에 큰 관심을 보이고 있습니다.맥킨지(McKinsey)의 최근 연구[2]에 따르면, 생성형 AI는 비기술 직군에서도 쉽게 접근할 수 있는 기술이며, 이는 보안 산업에 큰 잠재력을 제공합니다.

즉각적인 효율성과 보안을 동시에 향상시키는 활용 사례 중 하나는 이상 징후 감지 (Anomaly Detection)입니다. 이 기술은 기존의 규칙 기반 프로그래밍에서 생성형 AI를 활용한 딥러닝으로 발전하고 있으며, 영상 감시 분야에서 생성형 AI 알고리즘은 '정상적인' 장면을 학습하고, 실시간으로 발생하는 상황을 이해할 수 있는 특정 변화를 식별합니다.

예를 들어, 어두운 옷을 입은 사람이 제한 구역에 진입하는 상황을 인식할 수 있습니다. 이러한 알고리즘은 인간 에이전트가 오프라인에서 세밀하게 조정한 후, 엣지(Edge) 기능을 갖춘 여러 대의 카메라에 다시 배포할 수 있습니다. 오디오 감지 분야에서도 유사한 발전이 이루어지고 있습니다. 이상 음향을 감지하는 기능은 몇 년 전부터 존재했지만, 이제는 AI 가상 에이전트가 그 이상 음향이 무엇인지, 차량인지 장비인지 식별할 수 있습니다. 이를 통해 인간 보안 담당자는 즉각적인 대응이 가능한 정보를 얻을 수 있습니다.

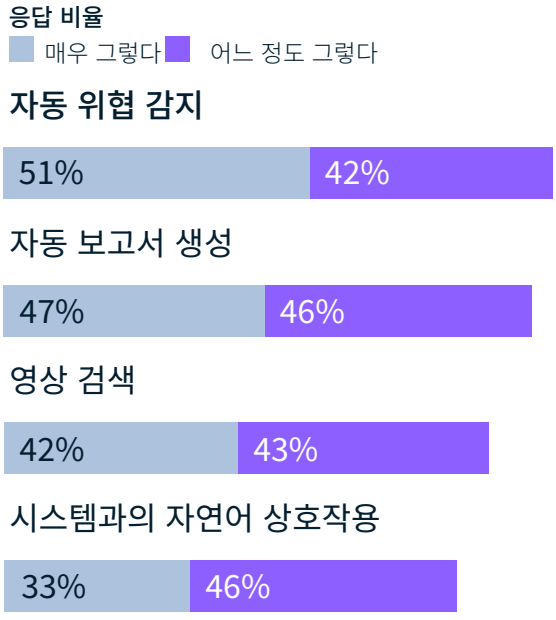
AI가 보안 응용 분야에 미치는 영향

AI는 기존의 보안 기술에서도 기능을 한층 강화하고 있습니다. 예를 들어, 생체 인증을 위한 얼굴 인식 기술은 오랫동안 사용되어 왔지만, AI는 사람의 외모 변화를 지속적으로 학습함으로써 인증의 정확성과 신뢰성을 높입니다.

통합 보안 관리에서도 동일한 효과가 나타나고 있습니다. AI는 여러 출처의 데이터를 통합하고 분석하여 잠재적인 문제를 나타낼 수 있는 패턴이나 추세를 인식할 수 있습니다. 예를 들어, AI는 특정 요일이나 시간대에 오경보(False Alarm)가 더 자주 발생한다는 사실을 파악할 수 있습니다. 또는 소매 업계에서는 특정 직원이 근무할 때 비정상적인 판매 거래(Point-of-Sale Transaction)가 발생하는 패턴을 식별할 수 있습니다. 이러한 인사이트는 보안 관리자가 오경보 관리부터 내부 절도 방지까지 다양한 문제를 해결하는 데 실질적인 도움을 줍니다.

AI는 보안 전문가들에게 새로운 가능성을 열어주고 있으며, 그 중요성은 앞으로 더욱 커질 것입니다. 그러나 각 조직은 보안 및 비즈니스 가치를 강화하기 위해 AI를 적용할 때 신중해야 하며, AI와 관련된 윤리적·규제적 요구 사항의 변화에도 주의를 기울여야 합니다.

조직들은 생성형 AI(GenAI) 도입을 준비하고 있습니다[1]



[1]2025년 2~3월에 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술 의사결정권자 575명을 대상으로 실시된 제3자 블라인드 설문조사.

[2]생성형 AI의 인간적 측면: 생산성 향상의 길을 찾다." 맥킨지 쿼터리, 2024년 3월 18일. https://www.mckinsey.com/capabilities/people-and-organisational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

Partner Insight

AI를 더 스마트하게 활용하기

AI가 앞으로도 보안과 감시 산업을 계속 변화시킬 것이라는 예측은 이제 놀라운 이야기가 아닙니다.

AI 기술은 이미 많은 조직의 감시 로드맵에서 핵심 요소로 자리 잡고 있으며, AI를 오디오 및 비디오 분석 기술과 결합함으로써, 더 높은 정확도의 객체 감지 및 분류가 가능해지고, 오경보(False Alarm)를 줄이는 동시에 고객이 실질적인 데이터를 기반으로 지능형 모니터링을 수행하고 운영 효율성을 향상시키며, 데이터 기반 비즈니스 인사이트를 얻을 수 있게 되었습니다.

하지만 이제 AI가 더 이상 '신흥 기술'의 단계를 넘어선 만큼, 업계가 던져야 할 질문은 다음과 같습니다.
"어떻게 하면 AI를 새로운 방식으로 활용하여 단순한 보안을 넘어, 조직의 미래 방향성에 영향을 미칠 수 있을까?"

앞으로는 오픈 플랫폼과 생성형 AI(Generative AI) 모델이 더욱 발전하면서, 장비와 '대화'하듯 명령을 내릴 수 있는 정밀한 기능이 구현될 것입니다. 예를 들어, "로비 카메라에서 새벽 1시부터 2시 사이에 빨간 셔츠를 입은 남성을 감지해줘."와 같은 구체적인 명령이 가능해질 것입니다.

또한 영상 보안 시장은 다른 보안 분야보다 빠르게 성장하고 있으며, AI 기술의 발전은 제조업체들이 자사 제품군 대부분에 AI를 어떻게 통합할지를 다시 설계하도록 만들고 있습니다.

보안 업계는 협력하여 AI와 관련된 가이드라인과 기준을 수립해야 하며, 대부분의 보안 및 감시 응용 분야에서 수용 가능한 정확도의 수준을 정의해야 합니다. 이는 최종 사용자, 유통업체, 제조업체 모두에게 유익합니다. 카메라에 대한 표준이 존재하듯 AI 정확성에 대한 표준 역시 마련되어야 합니다.

AI와 지능형 분석(Intelligent Analytics)의 결합은 보안 전문가들이 보다 안전하고 효율적인 감시 환경을 설계하고구축할 수 있도록 돕습니다. AI 기반의 지능형 기술이 계속 발전하면서, 단순한 보안 도구를 넘어 통합 비즈니스 솔루션으로 진화하고 있습니다.

업계가 던져야 할 질문은 명확합니다. **"AI를 어떻게 새로운 방식으로 활용하여 단순한 보안을 넘어 조직의 미래를 변화시킬 수 있을까?"**

Partner Insight

Honeywell

출입 통제 분야의 AI 응용프로그램

산업별 요구와 기술 발전에 대응하여, 여러 산업 분야에서 AI 기반 보안 및 안전 시스템의 도입이 빠르게 이루어지고 있습니다. 특히 헬스케어, 리테일, 제조업, 데이터 센터 산업에서 보안을 위한 AI 솔루션이 가장 빠르게 통합되고 있습니다.

예를 들어, 병원과 의료 시설에서는 AI 기반 보안 시스템을 통해 환자 안전을 강화하고 시설 출입을 보다 효과적으로 모니터링합니다.

데이터 센터에서는 AI 기반 예측 유지보수 및 보안 모니터링 시스템, 전자 출입 통제, 생체 인식, AI 보안 카메라 등이 활용되어 물리적 시설의 보안을 강화하고 있습니다.

AI 기술은 보안 모니터링과 사고 대응 역량을 강화하는 방향으로 더욱 고도화되고 있습니다. 최근 실시한 조사에서, 보안 및 거주자 안전은 현재 건물 내에서 AI가 가장 활발히 활용되는 주요 분야 중 하나로 나타났습니다.

60% 이상의 응답자가 AI를 이상 징후 감지에 사용하고 있으며, 절반 이상은 위치 추적용으로, 45%는 생체 인식 기반 출입 통제 시스템에 AI를 활용하고 있습니다.

또한 AI는 출입 이벤트, 영상 이벤트, 알람 등 다양한 출처의 데이터를 통합 및 분석하는 데 사용될 수 있습니다.

건물 보안을 위한 조직의 AI 활용 사례 (Security)

이상 징후 감지	→ 60%
위치 추적	→ 50%
생체 인식 기반 출입 통제	→ 45%

AI는 이러한 데이터를 통해 명확하게 드러나지 않는 데이터 간의 연관성을 찾아내어 보안 취약점을 예측할 수 있습니다. 이를 통해 보안 전문가들은 보다 사전에 위험을 파악하고 대응할 수 있게 됩니다.

이러한 방식으로 AI는 보안팀이 끊임없이 변화하는 위협 환경에 한 발 앞서 대응할 수 있도록 돕습니다. 또한 시스템의 취약점을 감지하고, 자동 패치 관리 (Automated Patch Management)를 통해 시스템 중단을 방지하는 데에도 활용됩니다.

Honeywell은 Wakefield Research에 의뢰하여 Honeywell Building Managers Research Survey를 진행했습니다. 이 조사는 미국 내 사무실, 병원, 공항, 학교, 대학, 호텔, 데이터 센터 등 다양한 건물 유형의 관리자 및 의사결정권자 250명을 대상으로 실시되었습니다. 응답자들은 모두 250명 이상의 입주자가 있는 건물에서 AI 기반 시설 관리 시스템을 사용 중이었습니다.

[1]mckinsey.com/capabilities/people-and-organisational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

클라우드 애플리케이션: 새로운 표준으로 자리 잡다

통합 보안 산업은 최근 몇 년간 클라우드 기반 솔루션의 급격한 확산으로부터 큰 혜택을 받고 있습니다. 확장성(Scalability), 구현의 간소화, 유지보수의 용이성, 그리고 사이버 위생(Cyber Hygiene)의 개선이 대표적인 장점입니다.

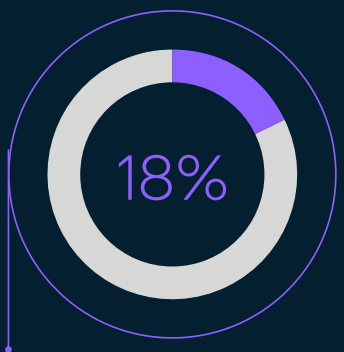
또한 전 세계적으로 데이터 센터 인프라가 빠르게 확장되면서, 이러한 솔루션은 이제 다양한 형태의 조직과 여러 보안 활용 사례(Security Use Cases)에 폭넓게 적용되고 있습니다.

현재 클라우드 기반 보안 기술은 완전히 성숙한 단계에 도달했으며, 많은 조직의 미래 보안 계획에 포함되어 있습니다.

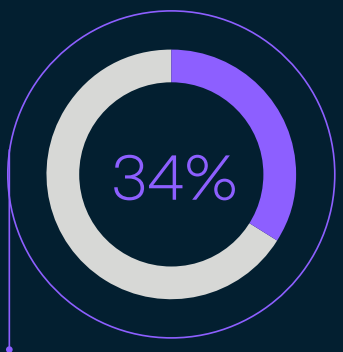
시장 조사에 따르면, 18%의 조직이 이미 완전한 클라우드 기반 보안 시스템을 운영 중입니다[1].

클라우드 도입은 계속 증가하고 있습니다[1]

조직 내 클라우드 기반 SI 기술 활용 현황:



현재 완전히 클라우드 기반으로 운영 중



향후 5년 내 완전한 클라우드 전환을 예상

[1]2025년 2월~3월에 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술 의사결정권자 575명을 대상으로 실시된 제3자 블라인드 설문조사.

데이터 최적화와 비용 효율성에 대한 요구

이제 진정한 엔터프라이즈급(Enterprise-Level) 클라우드 솔루션이 등장했습니다. 당사의 전략적 기술 파트너는 클라우드 데이터 인프라에 대규모 투자를 진행 중이며, 다른 첨단 기술 분야에 필적하는 수준의 발전을 이루고 있습니다.

이는 전 세계적으로 보안 기술을 관리하는 기업들도 물리적 보안 애플리케이션의 기본 플랫폼으로 클라우드를 활용할 수 있게 되었으며, 필요에 따라 프라이빗 클라우드(Private Cloud)도 선택지로 제공되고 있습니다.

또한 영상 감시, 출입 통제, 침입 감지 등 점점 더 다양한 보안 애플리케이션이 클라우드 환경에서 제공되어 감에 따라 클라우드 투자도 함께 확대되고 있습니다. 따라서, 데이터 저장 및 처리에 필요한 대역폭 비용은 점차 낮아지고 있습니다.

이로 인해, 방대한 데이터를 처리해야 하는 대표적인 기술인 영상 감시 분야에서 새로운 혁신이 촉진되고 있습니다. 카메라 제조업체들은 영상 압축 알고리즘(Video Compression Algorithm)의 개선에 집중하고 있으며, 비트레이트와 저장 비용을 크게 줄임으로써 클라우드 기반 및 AI 기반 영상 플랫폼의 도입을 가속화할 것입니다.

하이브리드 클라우드: 안정적인 전환 단계

클라우드 솔루션이 보안의 주류(Mainstream)로 자리 잡으면서, 하이브리드 접근법은 완전한 클라우드 기반 보안 기술로 전환하는 조직에게 안정적인 중간 단계가 되고 있습니다.

> “클라우드 기술은 조직이 보안을 원격으로 관리하고, 필요에 따라 인프라를 확장하며, 여러 보안 기능을 하나의 통합 플랫폼으로 관리할 수 있도록 합니다.”
>
> 3xLOGIC

조직은 기존 온프레미스(On-Premises) 시스템을 수명 종료 시점까지 사용하면서도, 점진적으로 클라우드 기반 시스템을 확대할 수 있습니다.
하지만 온프레미스 인프라 운영에는 유지관리 부담과 규제 준수 비용이 수반되며 동시에 이에 대한 비용도 점점 높아지고 있음을 확인하고 있습니다. 이러한 비용을 모두 고려했을 때, 클라우드 솔루션은 총소유비용 (TCO, Total Cost of Ownership) 측면에서 훨씬 더 매력적인 선택입니다.

시장 조사 결과, 클라우드 도입을 이끄는 주요 요인은 유지관리의 용이성, 중앙 집중형 관리, 운영 비용 절감, 그리고 효율성 향상으로 나타났습니다. 이러한 이점들은 무시하기 어려운 강력한 이점입니다.

클라우드 기술 도입이 늦은 기업들에게도 희소식은, 데이터 보안, 개인 식별 정보(PII)의 보호, 시스템 복원력 확보를 위한 모범 사례(Best Practice)가 이미 충분히 구축되어 있다는 점입니다.
Securitas Technology와 같은 보안 통합 업체들은 조직이 클라우드 기반 기술을 원활하게 도입할 수 있도록 명확한 계획을 수립하는 데 중요한 역할을 하게 될 것입니다.

일부 조직은 여전히 온프레미스 기술을 유지하고, 다수의 기업은 하이브리드 방식을 선택하겠지만, 추세는 분명합니다. 클라우드 기술은 앞으로 보안 분야의 필수적인 요소가 될 것입니다.

brivo
simply better security

Partner Insight

클라우드 기반 보안 시스템으로의 전환

조직들이 클라우드로 시스템을 빠르게 이전하는 데에는 분명한 이유가 있습니다.클라우드 기반 보안 기술은 원격 접근(Remote Access)과 관리 기능을 제공하여, 기업이 언제 어디서나 시설을 모니터링하고 제어할 수 있도록 합니다.

클라우드 네이티브 솔루션(Cloud-Native Solution)을 통해 새로운 기술을 확장하고 연결하는 과정이 훨씬 간단해졌으며, 온사이트 서버, 유지보수, IT 지원에 드는 비용을 절감시켜, 기업은 시스템 관리보다는 핵심 비즈니스 우선순위에 더 많은 자원을 집중할 수 있도록 합니다.

그러나 명확한 장점에도 불구하고, 여전히 많은 조직은 기존 하드웨어 투자에 대한 우려로 인해 전환을 망설이고 있습니다.

예를 들어 온프레미스 제어판(On-Premises Control Panels)과 하위 장치(Downstream Devices)는 어떻게 될까요?
이러한 문제를 해결하기 위해 Brivo Mercury 솔루션은 기존 Mercury 제어판을 클라우드 환경으로 손쉽고 경제적으로 전환할 수 있도록 지원하며, 이 과정에서 운영 중단을 최소화합니다.

> “하이브리드 VMS 솔루션은 내장된 사이버 보안 기능을 통해 규정 준수, 복원력, 데이터 보호를 보장합니다.”

이 접근 방식은 비용이 많이 드는 ‘전면 교체(Rip-and-Replace)’없이도 클라우드의 장점과 현대적인 보안 시스템을 제공합니다.보안 시스템을 현대화하면 중앙 집중화의 가치를 극대화할 수 있습니다.

예를 들어 Brivo Security Suite와 같은 통합 보안 플랫폼은 출입 통제, 영상 인텔리전스, 방문자 관리, 침입 감지 기능을 하나의 대시보드에서 관리할 수 있게 합니다.

중앙 집중형 클라우드 기반 플랫폼은 모든 보안 기능을 하나의 인터페이스로 통합하여, 모든 위치의 상황을 한눈에 볼 수 있는 ‘단일창(Single Pane of Glass)’ 환경을 제공합니다. 이를 통해 여러 플랫폼과 도구를 병행 운영해야 하는 번거로움을 줄이고, 사이버 보안을 더욱 강화할 수 있습니다.

또한 클라우드 기반 보안을 통해 조직은 비즈니스 시스템과 통합된 실시간 보안 지표 및 정보를 확보하여, 보다 빠르고 정확한 의사결정을 내릴 수 있습니다.

Partner Insight

영상 감시의 미래: 하이브리드 VMS가 여는 확장성과 유연성

빠르게 변화하는 기술 환경 속에서 기업들은 확장성과 유연성을 모두 갖춘 감시 솔루션을 찾고 있습니다.

하이브리드 영상 관리 시스템(VMS, Video Management System)은 클라우드와 온프레미스(On-Premises) 배포의 장점을 결합해 다양한 요구를 충족시키는 영상 보안의 진화를 보여줍니다.

Milestone의 XProtect와 Arcules의 조합과 같은 하이브리드 VMS 솔루션은 클라우드 인프라를 활용하여 탁월한 확장성을 제공합니다.
이를 통해 기업은 영상 감시 역량을 원활하게 확장하고, 조직의 성장에 따라 증가하는 데이터 저장 및 처리 요구를 유연하게 대응할 수 있습니다.

또 다른 장점은 유연성입니다. 기업은 순수 클라우드, 엣지 클라우드, 카메라-투-클라우드 등 다양한 배포 옵션을 선택하여 필요에 맞게 보안 시스템을 맞춤 구성할 수 있습니다. 이 솔루션은 온프레미스 시스템과 통합될 수 있으며, 견고한 보안이든 민첩한 클라우드 운용이든 자유롭게 조정할 수 있습니다.

또한 하이브리드 VMS 솔루션은 내장된 사이버 보안 기능으로 설계되어, 규정 준수와 복원력, 데이터 보호를 보장합니다.
이러한 '보안 중심 설계(Secure-by-Design)' 접근 방식은 영상 데이터가 잠재적 위협으로부터 안전하게 보호된다는 신뢰를 제공합니다.

클라우드와 온프레미스 시스템의 통합은 비즈니스 인텔리전스를 강화합니다.

Arcules의 고급 분석(Analytics) 및 인공지능(AI) 기능과 결합된 영상 데이터를 활용하면, 보안과 운영 효율성을 향상시키는 빠르고 정확한 의사결정을 내릴 수 있습니다.
이러한 미래 대응형 기능(Future-Proofing)은 보안 시스템이 변화하는 수요 속에서도 지속적으로 관련성을 유지하도록 합니다.

결론적으로, 하이브리드 VMS의 확장성과 유연성은 영상 감시 산업의 혁신을 이끌고 있으며,
Milestone의 XProtect와 Arcules와 같은 솔루션은 배포의 자유, 강력한 보안, 향상된 비즈니스 인텔리전스를 제공하며, 적응력 있고 탄력적인 미래를 위한 기반을 마련합니다.

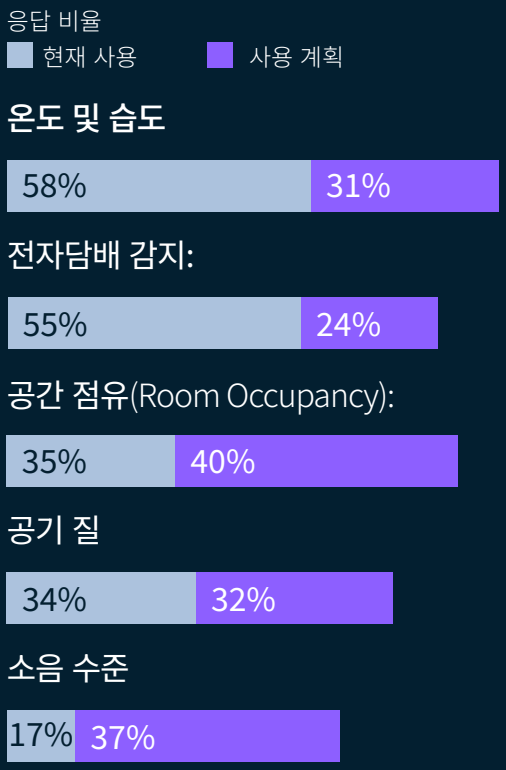
진화하는 고급 센서 기술의 활용

고급 센서 및 기타 연결 장치(일명 사물인터넷, IoT)의 잠재력은 보안 업계에서 오랫동안 큰 관심을 받아왔습니다. 침수, 온도 및 조도, 공기 질, 소리, 흡연 및 전자담배 감지 등 개별 장치의 기술은 이미 널리 사용되어 있습니다.

설문조사에 따르면, 61%의 조직이 보안 시스템에 고급 센서를 통합한 것으로 나타났습니다.

그동안 업계는 단순히 경보(Alert)를 전송하는 수준을 넘어 보안 강화나 운영 효율성을 높이는 실질적 가치를 제공하는 데 어려움을 겪어왔습니다. 하지만 이제 이러한 상황이 변화하기 시작했습니다.

더 많은 것을 모니터링하기[1]



[1]2025년 2월~3월, 호주 · 프랑스 · 독일 · 스웨덴 · 영국 · 미국에서 보안 기술 의사결정권을 가진 보안 전문가 575명을 대상으로 실시한 제3자 블라인드 설문조사.

감시 카메라의 다중 센서화

인공지능(AI)과 데이터 분석 기술의 발전 덕분에, 이제는 별도의 센서 장치 없이도 다양한 형태의 환경 모니터링을 능동적으로 수행할 수 있게 되었습니다.

영상 보안 기술의 혁신이 대표적인 예입니다. AI 기능이 내장되어 있거나('엣지 컴퓨팅') 영상 분석 소프트웨어와 연결된 카메라는 이제 다중 센서 장치(Multi-Sensor Device) 로 활용되고 있습니다.

시간에 따라 장면을 모니터링하면 AI 알고리즘은 단순한 보안 위협뿐만 아니라 연기, 화재, 동물, 군중, 심지어 총성과 같은 예기치 않은 환경 변화도 감지할 수 있습니다. 영상 시스템을 지능형 다중 센서로 활용하면, 정밀한 정보를 인간 에이전트에게 전달하여 대응을 자동화(Automated Response) 할 수 있습니다.

센서 통합을 통한 비즈니스 가치 창출

보안 및 환경 모니터링은 외부 위협 관리에만 국한되지 않습니다. 센서를 보안 시스템과 통합해 수집된 데이터를 활용하면, 건강·안전·업무 효율성을 최적화하여 비즈니스 가치를 높일 수 있습니다.

소매업의 경우, 보안 및 환경 센서를 결합하면 고객 행동에 대한 핵심 인사이트를 얻을 수 있습니다. 예를 들어, 매장 내 점유율(Room Occupancy)을 추적하거나 고객 이동 경로를 파악함으로써 향후 마케팅 전략에 유용한 데이터를 확보할 수 있습니다.

센서 통합을 통한 비즈니스 가치 창출시장 조사 결과, 전체 조직의 약 3 분의 1(37%)이 소음 수준을 모니터링하기 위해 센서를 활용할 계획이 있는 것으로 밝혀졌습니다[1]. 이 애플리케이션은 소음이 직원이나 고객에게 부정적인 영향을 미칠 수 있는 다양한 산업 분야에서 특히 중요한 역할을 합니다. .

예를 들어 제조업에서는 센서가 산업 기계의 과도한 소음으로부터 근로자를 보호할 수 있습니다. 또한 온도와 습도를 모니터링하기 위한 환경 센서, 열화상 카메라, 영상 분석 기술의 활용이 점점 증가하고 있으며, 이는 생산 감독자가 장비 과열을 조기에 감지할 수 있도록 돕습니다.

호환성과 사이버 보안의 균형

센서 간의 호환성 향상은 SI 플랫폼 내 센서 통합을 지속적으로 촉진할 것으로 예상됩니다.
이를 통해 조직은 보다 광범위하게 연결된 비즈니스 환경 모니터링 생태계를 구축할 수 있습니다.

어떤 환경 센서나 기타 연결 장치를 사설 보안 네트워크에 통합할지 고려할 때, 조직은 보안 기술 공급업체와 긴밀히 협력하여, 공급업체의 제품을 평가하고, 장치가 품질·지원·사이버 보안 측면에서 요구되는 기준을 충족하는지 확인하는 것이 중요합니다.

Partner Insight

카메라를 강력한 알람 감지 장치로 전환하기

분석 소프트웨어의 빠른 발전으로 기존의 영상 감시 카메라에도 고급 분석 기능을 적용할 수 있게 되었습니다.

DMP의 XV 게이트웨이(XV Gateways) 와 AlarmVision® 솔루션은 표준 IP 카메라를 강력한 경보 감지 장치로 전환시킵니다. 움직임 감지(Motion Detection)를 분석 기능으로 강화하고, 영상 이벤트를 침입 경보 패널과 매끄럽게 통합함으로써, 조직은 즉각적인 알림을 통해 모든 상황을 실시간으로 파악할 수 있습니다.

오경보(False Alarm) 감소

카메라와 침입 감지 패널 간의 직접적인 통신은 카메라를 지능형 동작 감지 장치로 전환시켜, 자동으로 행동이나 알람을 트리거할 수 있게 합니다.

영상 분석을 통해 움직임의 주체를 사전에 식별하여 경보를 전송함으로써, 최종 사용자가 영상을 검증하고 모니터링 센터의 영상 검증의 정확도를 높일 수 있습니다.

빔(Beam) 대체 기능

감지를 위해 빔을 설치하는 것은 시간과 자원이 많이 들 뿐 아니라, 종종 불안정하고 비용이 큰 오경보를 유발하는 문제가 있습니다.

하지만 카메라를 포함한 보안 시스템은 이러한 감지 빔을 효과적으로 대체할 뿐 아니라, 그 이상의 기능을 제공합니다.

카메라를 침입 제어 패널과 통합하면, 카메라는 특정 구역별로 작동하는 강력한 경보 장치로 전환됩니다. AlarmVision® 의 경우, 카메라당 최대 네 개의 구역을 맞춤 설정할 수 있습니다.

계절별 유연성(Seasonal Flexibility)

또 다른 장점은 계절별 활동이나 환경 변화에 유연하게 대응할 수 있다는 점입니다.

현장을 직접 방문하거나 추가 인력을 투입해 빔이나 배선을 옮길 필요 없이, 카메라 구역을 빠르고 쉽게 조정할 수 있습니다.

계절별로 활동이나 재고가 변동될 수 있지만, AlarmVision® 과 같은 고급 솔루션은 이러한 보호 절차를 훨씬 간소화할 수 있습니다.

Partner Insight

resideo

연결형 보안 센서: 보안 환경의 혁신

스마트 기술이 우리의 삶 전반을 변화시키고 있는 오늘날, 보안 시스템도 예외가 아닙니다.
Resideo는 ProSeries 연결형 보안 센서(Connected Security Sensors)를 통해 보안 산업의 혁신을 주도하고 있습니다.
이 혁신적인 장치는 가정, 기업, 그리고 보안 전문가들이 안전과 보안을 접근하는 방식 자체를 새롭게 바꾸고 있습니다.

ProSeries 센서는 첨단 기술을 통해 메인 패널과 모바일 장치 간의 원활한 통신(Seamless Communication)을 가능하게 합니다.
이 연결성은 센서의 성능을 향상시키고, 실시간 업데이트 및 원격 기능을 제공하여 사용자에게 보안 시스템에 대한 전례 없는 수준의 제어를 제공합니다.

ProSeries 센서는 다양한 옵션을 제공하며, 모든 센서에는 향상된 암호화(Enhanced Encryption), 오경보 감소, OTA 업데이트와 같은 고급 기능이 탑재되어 있습니다. 쉽게 연결되어 완전한 통합형 생태계(Integrated Ecosystem) 를 형성할 수 있습니다.

연결성은 센서의 성능을 향상시키고, 실시간 업데이트와 원격 기능을 제공하며 사용자에게 보안 시스템에 대한 전례 없는 수준의 제어를 제공 합니다.

가정이나 기업 소유자가 업무 중 알림을 받고, 원격으로 자산을 모니터링할 수 있도록 함으로써, 보다 능동적이고 즉각적인 보안 관리가 가능합니다.
또한 이 시스템은 클라우드 기반 기술을 활용하여 관리와 문제 해결을 용이하게 하고, 다운타임을 줄이며 시스템 신뢰성을 향상시킵니다.

무선 통신과 데이터 암호화 기술의 지속적인 발전은 ProSeries 센서가 효율적일 뿐만 아니라 높은 수준의 보안성(Security) 을 갖추도록 보장합니다.
Resideo는 사물인터넷(IoT)을 적극적으로 도입하고, 유연하고 확장 가능한 솔루션을 제공함으로써 보안의 새로운 가능성을 넓히고 있습니다.

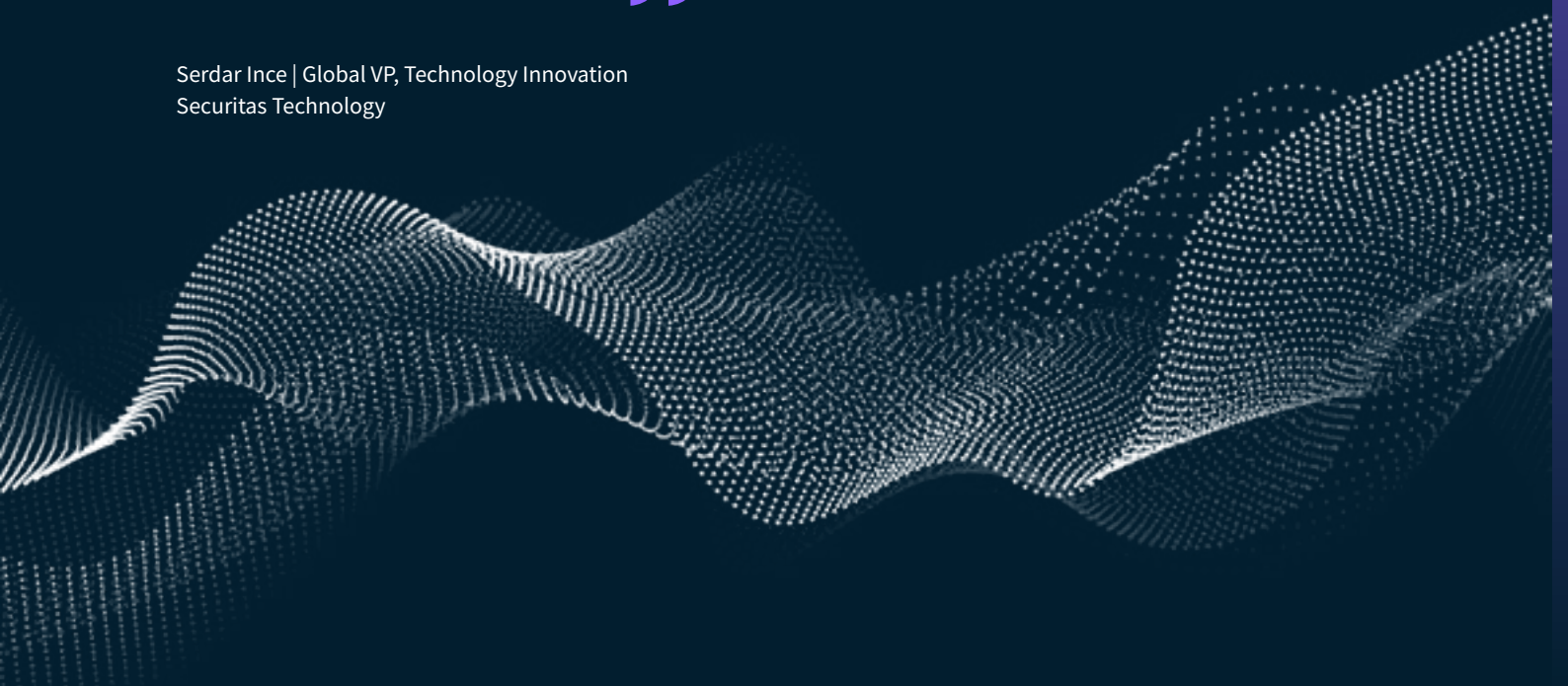
ProSeries 연결형 센서는 보안 시스템의 혁신적 도약으로, 더 스마트하고 사용자 친화적이며 오늘날 변화하는 보안 환경에 보다 효과적으로 대응할 수 있는시스템으로 진화시키는 획기적인 도약입니다.

보안 전문가를 위한 실행 계획

"GenAI(생성형 인공지능)는 영상 분석 방식을 근본적으로 변화시킬 것입니다. 고객은 더 세밀하게 상황을 분석하고 즉각적인 인사이트를 얻을 수 있습니다.

클라우드 기술과 결합하면, 모든 데이터를 더욱 효율적으로 처리하고 관리할 수 있습니다. 또한 고급 센서의 호환성이 높아짐에 따라, 비즈니스 효율성과 인텔리전스를 강화하는 연결형 생태계(Connected Ecosystem) 를 통해 보안의 범위를 한층 확장할 수 있습니다."

Serdar Ince | Global VP, Technology Innovation
Securitas Technology



인공지능

1

AI 데이터 전략 수립

AI가 해결할 수 있는 데이터 소스와 보안 과제 또는 기회를 식별합니다. 예시로는 객체 감지(Object Detection) 및 추적, 차량 인식, 이상 징후 감지(Anomaly Detection) 등이 있습니다. 명확한 목표를 설정하면 AI 활용이 조직의 전체 보안 전략과 목적에 부합하도록 할 수 있습니다.

2

규제·법률·윤리적 요구사항 이해

법무팀과 협력하여 AI 애플리케이션이 관련 규제 및 데이터 개인정보 보호법을 준수하도록 합니다. AI 사용의 윤리적 영향을 고려하고, 책임 있는 사용을 위한 거버넌스 프로세스(Governance Process) 를 구축해야 합니다. 이는 신뢰를 형성하고 정보를 보호하는 데 도움이 됩니다. 또한, 다기능 AI 검토 위원회(AI Review Committee) 를 공식적으로 구성하여 명확하고 준수 가능한 AI 가이드라인을 수립하고 올바르게 시행되도록 지원할 수 있습니다.

클라우드 애플리케이션

3

클라우드 전환 모델 및 로드맵 구축

보안 운영을 클라우드로 이전하기 위한 명확한 전환 모델(Migration Model) 과 로드맵을 수립하고, 일정 및 주요 마일스톤을 정의하며, 보안 기술 파트너와 협력하여 향후 보안 요구에 맞는 클라우드 기반 솔루션과 서비스를 확인합니다.

4

전문 IT팀과 협업

IT 부서와 협력하여 그들의 전문 지식을 활용하고, 클라우드 기반 보안 기술 모델을 공동으로 설계합니다.

이 과정에는 인프라 요구사항 식별, 사이버 보안 위험 평가, 사이버 위생 프로세스(Cyber Hygiene Processes) 구축이 포함됩니다.

고급 센서

5

센싱(Sensing) 요구사항 정의

규제 준수, 효율성 향상, 직원 및 고객 경험 개선 등 보안 및 비즈니스 목표를 지원하는 특정 센서 애플리케이션과 환경 조건을 식별합니다.

그 후, 보안 기술 파트너와 협력하여 기존 보안 인프라에 고급 센서를 통합할 최적의 방식을 결정합니다.

6

공급업체 및 장치 호환성 검증

잠재적인 공급업체와 기술을 철저히 평가하여 품질, 규정 준수, 사이버 보안 기준을 충족하는지 확인합니다.

엔드포인트 보안(End-point Security), 알려진 취약점, 데이터 저장 방식 등을 평가하여 강력한 보호(Protection) 와 원활한 통합을 보장합니다.

3

불안정한 환경을 위한 보안 솔루션

코로나19 팬데믹 이후, 사회와 보안 전문가들은 증가하는 불안정성(Volatility)에 대응해 왔습니다.

오늘날 이러한 추세는 둔화 되지 않고, 지정학적 긴장, 경제적 불확실성, 극단적인 기후 현상 등으로 인해 세계 여러 지역에서 불안정성이 더욱 증가하고 있습니다.

보안 전문가는 직장 내 사고, 사회적 불안, 자연 재해 등 가능성은 낮지만 영향력이 큰 다양한 사건에 미리 대비해야 합니다.

또한, 당사의 클라이언트 자문위원회(Client Advisory Board) 역시 동일한 우려를 표했습니다. 예측 불가능한 비즈니스 환경속에서, 직원과 시설, 자산을 보호하는 것이 점점 더 어려워지고 있다고 밝혔습니다.

모든 환경에서 안전을 향상하는 기술

새로운 기술들은 사무실, 원격 근무지, 은행, 매장, 학교 등 다양한' 환경에서 사람의 안전을 개선하도록 돕고 있습니다. 이 섹션에서는 조직이 어떤 상황에도 대비 할 수 있도록 어떤 혁신적인 방법을 모색하고 있는지 살펴봅니다.

직원 안전은 가장 중요한 투자 요인입니다[1]

설문조사 응답자의 다수가 직원 안전을 보안 기술 투자 상위 3대 요인으로 꼽았으며, 30%는 최우선 요인으로 선정했습니다.

더 많은 위험을 감시하기 위한 모니터링

AI, 클라우드 애플리케이션, 그리고 첨단 센서 기술의 발전으로 인해 보안 전문가는 조직의 근무 환경을 다양한 안전 및 보안 위험으로부터 감시할 수 있는 새로운 방법들을 계속해서 발견하고 있습니다. 그 예시는 다음과 같습니다.

- **경계 구역을 넘어서는 보호:**

  라이다(LiDAR, 광 감지 및 거리 측정)를 기존의 침입 감지 시스템에 통합하여, 외부 경계뿐 아니라 창고와 같은 내부 시설과 같이 넓은 지역에서도 사전 대응, 실시간, 고정밀 감지가 가능합니다.

- **의심스러운 소리에 대한 대응:**

  다중 센서 장치나 AI 기반 영상 감시 스템에 내장된 오디오 분석 기술은 단순히 소리를 감지하는 것을 넘어 이를 분류하여, 인식과 대응 능력을 향상시킵니다. 예를 들어, 오디오 분석 기능이 탑재된 영상 시스템은 교통 소음과 같은 일상적인 소리를 걸러내고, 총성이나 "도와줘!" 같은 비상 신호를 즉시 감지하도록 설정할 수 있습니다.

- **환경 조건 감지:**

  환경 센서를 SI 시스템에 통합하여, 조직은 주변 환경의 미묘한 변화까지 감지하고 이에 대응할 수 있습니다. 대표적으로 무단 흡연 및 전자담배 사용, 공기 중 유해 화학물질의 존재, 갑작스러운 온도 변화, 공격적인 행동의 소리 등이 포함됩니다.

[1]본 조사는 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술 의사결정권자 575명을 대상으로 2025년 2~3월에 진행된 제3자 블라인드 설문조사 결과입니다.

비상 상황 효율적으로 관리하기

조직의 보안 프로그램에서 효과적인 사고 대응 관리는 단순한 업무 중단과 심각한 재난을 가르는 핵심 요소 입니다.

기업은 기술 솔루션을 활용하여 비상 상황과 사고 발생 시 즉각적인 대응 능력을 강화하고 있습니다.

- 학교나 캠퍼스 환경에서 일반적으로 사용되는 이 기술은 자연재해, 총기 난사 등과 같은 보안 및 안전 위험 상황을 실시간으로 다수의 사람들에게 경고할 수 있습니다. 모바일 기기, 음성 메시지, 기타 디지털 채널을 통해 즉각적으로 알림을 제공하며, 상황별 안전 지침, 대피 절차, 비상 대응 지시 등을 안내하여 안전한 이동을 돕습니다. 설문조사에서 응답자의 22%가 모바일 기기에 대한 대규모 알림 기술을 '향후 도입할 주요 5대 기술' 중 하나로 꼽았습니다[1].

- 긴급 대응 기관과의 정보 공유: 북미 지역에서는 고위험 조직이 보안 및 영상을 긴급 구조 기관과 직접 공유하는 사례가 늘어나고 있습니다.

  클라우드를 통해 주요 카메라 영상에 접근 권한을 공유함으로써, 구조 인력에게 향상된 상황 인식 능력을 제공하고 긴급 대응의 정확성과 속도를 높일 수 있습니다.



원격 서비스를 통한 중단 없는 보안 유지

최근 들어 많은 조직들이 보안 시스템의 안정적 운영과 성능 최적화를 위해 원격 관리 서비스를 도입하고 있습니다. 대표적인 서비스는 다음과 같습니다.

- 예방적 시스템 상태 모니터링: 보안 시스템의 상태와 성능을 최적화하도록 설계된 상시 관리형 서비스입니다. AI 도구와 전문 인력이 결합되어 배터리 고장, 카메라 시야 방해 등 잠재적 문제를 사전에 감지하고, 시스템 다운타임을 최소화합니다.

- 펌웨어 및 비밀번호 관리: 이러한 자동화된 원격 서비스는 보안 시스템이 IT 네트워크에 안전하게 연결되도록 유지하고 외부 사이버 위협으로부터 보호합니다.

- 원격 운영 보호: 자연재해나 물리적 접근이 제한되는 위기 상황에서도 원격 서비스는 시설 모니터링 및 보호에 필수적입니다. 직접 접근이 어려운 경우에도 원격 모니터링을 통해 시설 침입이나 약탈 행위 등 사고를 예방할 수 있습니다.

> "보안 제품은 이제 AI, 센서, 분석 기술을 통해 위협을 조기에 식별합니다. 통합 카메라, 출입 통제, 알람, 인터폰 시스템을 결합하여 신속하게 확인 및 대응합니다.
> 그 결과 감지와 대응 간의 지연이 줄어들고 피해를 최소화 할 수 있습니다."
>
> Resideo

Partner Insight

비즈니스 연속성을 위한 기술 전략

출입 통제 시스템은 고객 시설에 접근해야 하는 모든 사람의 안전과 보안을 보장하는 핵심 요소입니다.

이러한 시스템을 지속적이고 안정적으로 운영하기 위해서는 비즈니스 연속성 계획(Business Continuity Planning) 이 시스템 설계 단계에서부터 고려되고, 시스템 수명 전반에 걸쳐 지속적으로 관리되어야 합니다.

네트워크 설계 고려사항

임베디드 네트워크 출입 통제 장치는 기본적으로 독립형(stand-alone) 으로 설계되어 있습니다.
네트워크 장애가 발생하더라도 컨트롤러는 계속해서 출입 결정을 내리고 이벤트를 버퍼링할 수 있지만, 이벤트 및 경보는 운영자에게 전달되지 않을 수 있습니다.

복원력을 높이기 위해 컨트롤러는 주(primary) 및 보조(backup) 네트워크 포트를 모두 갖춰야 하며, 이 포트들은 온프레미스 또는 클라우드 환경의 시스템 헤드엔으로 서로 다른 네트워크 경로를 통해 연결되어야 합니다. 기본 네트워크가 실패할 경우, 보조 포트로 자동으로 전환되어 트래픽을 유지하고, 경보가 정상적으로 전달되도록 보장합니다.

온프레미스 시스템의 경우 헤드엔드(Head End) 구성도 중요합니다.
고가용성(HA) 설정을 통해 두 개의 서버 또는 가상 머신(VM)을 구성하여 백업 운영이 가능하도록 하십시오.
또한, 백업 서버를 다른 장소에 두되 가까운 거리에서 즉각적으로 전환(failover)이 가능하도록 설계하면 더욱 효과적입니다.
최고 수준의 복원력을 원한다면, 재해 복구(DR) 서버를 구축하여 HA 환경이 실패했을 때도 “웜(warm)” 전환이 가능하도록 해야 합니다.

클라우드 기반 시스템의 경우, 다중 가용 영역(multiple availability zones) 을 제공하는 공급자를 선택하여 단일 위치의 장애에 대비해야 합니다.
또한, 시스템 데이터베이스의 백업 전략이 철저히 구성되어야 하며, 최소한 매시간 정기 백업 및 복원 포인트를 유지해야 합니다.

제로 트러스트 네트워킹(Zero-Trust Networking) 은 특히 클라우드 기반 시스템에서 신뢰성과 복원력을 높이는 효과적인 방법입니다. 추가 네트워크 장치가 필요할 수 있으나, 사이버 공격에 대한 저항력이 향상됩니다.

운영 고려사항

비즈니스 연속성을 강화하려면 체계적인 사이버 위생 관리(Cyber Hygiene) 를 통해 잠재적 취약점을 사전에 방지해야 합니다.
컨트롤러와 헤드엔드 소프트웨어에 대해 정기적인 소프트웨어 업데이트와 침투 테스트를 실시하여 취약점을 식별하고 완화하십시오.

또한, 시스템의 정상적 작동을 능동적으로 사전에 모니터링하고 고장을 예측하며, 경고를 주는 것도 중요합니다.

하드 드라이브 용량이 한계에 다다랐는가? 네트워크 지연(latency)이나 재시도 횟수가 증가하는가? 데이터베이스 오류가 발생하는가?
이러한 작은 신호 하나하나가 큰 문제의 전조일 수 있습니다.

마지막으로, 배터리를 잊지 마십시오!
정기적으로 출입 컨트롤러의 백업 배터리를 점검하고 교체하여, 정전 시에도 시스템이 정상 작동하도록 유지해야 합니다.

Partner Insight

디지털 중심 출입 관리로 직장 보안 강화

직장 내 보안 위협이 진화함에 따라, 조직은 인력·자산·데이터를 효과적으로 보호하기 위해 출입 관리 전략을 현대화해야 합니다.

디지털 중심(Digital-First) 접근 방식은 보안을 강화하고 효율성을 높이며, 실시간 인텔리전스를 통해 위험을 선제적으로 완화할 수 있도록 합니다.

이 접근 방식은 모바일 출입증, 지능형 자동화, 분석 기술을 활용하여 원활하고 안전한 사용자 출입 경험을 제공합니다.

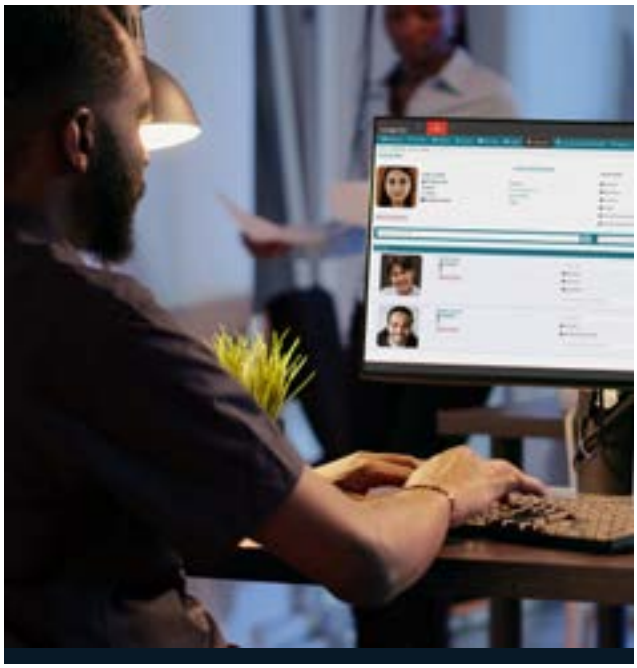
직원과 방문객은 스마트폰으로 출입이 가능하며, 분실 또는 도난된 카드로 인한 보안 위험을 최소화합니다.

또한 보안 담당자는 원격으로 권한을 관리하고, 접근 시도를 실시간으로 모니터링하여, 잠재적 위협에 신속하게 대응할 수 있습니다. 디지털 접근 관리의 또 다른 장점은 AMAG의 Symmetry CONNECT와 같은 신원 관리 솔루션(Identity Management) 과의 통합입니다.

출입 통제 시스템을 인사(HR) 및 IT 시스템과 연계하여, 조직은 보안 정책을 자동으로 적용하고 승인된 인원만 특정 구역에 접근할 수 있도록 보장할 수 있습니다.

조직은 직장 보호에 있어 선제적 보안 접근 방식을 도입해야 합니다.

디지털 중심 출입 관리는 변화하는 위협으로부터 직장을 보호하는 데 필요한 민첩성, 인텔리전스, 효율성을 제공하여 진화하는 위협으로부터 직장을 보호합니다. 이러한 첨단 기술을 수용함으로써, 기업은 운영 효율성을 높이는 동시에 더 안전하고 회복력 있는 근무 환경을 구축할 수 있습니다.



VERINT

Partner Insight

사기 예방을 위한 은행의 모범 사례

급변하는 환경 속에서 보안은 운영의 신뢰성과 고객 신뢰를 유지하는 핵심 축입니다.

은행은 대량의 민감 데이터를 다루기 때문에, 사이버 위협과 물리적 위협 모두를 포괄하는 통합 보안 접근법이 필요합니다.

IT 보안과 물리 보안 팀의 융합은 경쟁이 치열한 금융 시장에서 생존을 위한 필수 요소입니다.

기존의 IT와 물리 보안이 분리된 운영 방식은 더 이상 효과적이지 않습니다.

생체인식 출입 통제와 AI 기반 영상 감시와 같은 현대 기술은 통합적인 관리가 필요하며, 클라우드 기반 솔루션은 물리적 보안과 디지털 보안의 경계를 더욱 허물고 협업의 중요성을 부각시킵니다.

통합된 팀은 ATM 스키밍(카드 복제) 이나 디지털 계정 탈취 같은 복합 위협에 효과적으로 대응할 수 있습니다.

사전 감시 및 데이터 실시간 공유를 결합한 전략은 사기를 사전에 방지하는 데 도움을 줍니다.

또한, 사기 방지는 사람의 인식과 교육에도 의존합니다. 내부 위협은 심각한 문제이며, 은행은 직원이 내부 위험을 식별하고 대응할 수 있도록 교육과 프로그램을 정기적으로 운영합니다.

리더십은 통합적 접근을 이끌고 유연한 전략을 장려하는 핵심 역할을 하며, 새로운 기술과 조직이 직면한 특정 보안 과제에 대해 지속적인 교육이 필요합니다.

결국, IT와 물리 보안의 통합은 성공적인 은행 보안을 위한 핵심 요소이며,

다른 산업에도 적용 가능한 교훈으로, 사일로 구조를 제거하고 협업을 촉진하며 지속적인 교육을 강조합니다.

보안 통합에 성공한 은행들은 자산 보호, 고객 신뢰 유지, 변화하는 위험에 대하여 회복력 있게 대응하려는 다른산업에 귀중한 인사이트를 제공합니다.


Securitas
Technology

조직과 사람을 위한 준비 전략

최첨단 기술을 도입하는 것 뿐만 아니라, 조직은 고도화된 위협 예측 전략에 점점 더 많은 투자를 하고 있습니다. 사전 인텔리전스(Intelligence를 활용하고 철저한 사후 분석을 수행함으로써, 보안 전문가들은 미래의 보안 사건에 더 잘 대비하고 보호받을 수 있도록 노력합니다.

인텔리전스 기반 보안

오늘날 상호 연결된 세계에서, 불확실성(Volatility), 불안정성(Uncertainty), 복잡성(Complexity), 모호성(Ambiguity) — 즉 VUCA 환경은 지속적인 도전 과제입니다. 이러한 이유로, 조직이 위험보다 한 발 앞서 나갈 수 있도록 지원하는 상업적 리스크 인텔리전스 서비스 시장이 빠르게 성장하고 있습니다.

조사 결과, 응답자의 20%가 리스크 인텔리전스 서비스를 보안 프로그램에 통합할 계획이라고 답하며 높은 관심을 보였습니다[1].

리스크 인텔리전스 서비스는 보안 전문가들이 어느 영역에 보안 투자를 집중해야 할지를 판단하도록 돕습니다. 이 서비스는 정보를 활용하여 어느 지점이 더 큰 위험에 노출되어 있는지를 파악하고, 다음과 같은 기능을 통해 선제적(Preemptive) 보안 접근 방식을 가능하게 합니다:

- **위험 예측 보고서:** 매일, 주간, 월간 단위로 중요한 상황 인식 정보를 제공합니다. 이 보고서는 지역, 국가, 글로벌 수준의 인사이트를 제공하도록 설계되어 있으며, 조직이 잠재적 위험에 대비하도록 돕습니다.
- **범죄 지수 보고서:** 글로벌 및 국내 범죄 동향부터 지역 수준의 데이터까지 분석하는 첨단 기술 기반 서비스입니다. 인터랙티브 지도, 세부 통계, AI 기반 분석을 통해 조직이 사업을 운영하는 지역의 범죄 데이터를 비교, 연구, 예측할 수 있도록 지원합니다.

준비가 곧 안전강화의 핵심입니다

자연재해부터 화재, 직장 내 폭력에 이르기까지, 조직은 빠르게 비상사태로 확대될 수 있는 다양한 잠재적 위험에 직면해 있습니다. 위기 상황에서 침착하고 자신감 있게 대응하기 위해서는 철저한 사전 준비가 필수적입니다.

비상 대응 서비스에 대한 관심이 증가하고 있으며, 더 많은 조직이 직원과 직장의 안전을 보호하기 위한 사전적 대응 계획의 중요성을 인식하고 있습니다.

시장 조사에 따르면, **88%의 조직이 비상 상황에 대응하기 위한 공식 계획을 수립**했다고 답했습니다. 이는 많은 보안 전문가들이 이 분야를 중점적으로 다루고 있음을 보여줍니다[1].

하지만 18%의 조직은 자신들의 대비 수준에 대해 자신감이 낮거나 거의 신뢰하지 않는다고 응답했습니다. 따라서 이 부분은 모든 조직의 우선 과제가 되어야 합니다.

다음의 서비스들은 계획 수립부터 교육까지 다양한 방식으로 조직의 비상 대응 능력을 강화합니다.

- **비상 계획(Emergency Planning):** 조직 맞춤형 비상 대응 계획(EAP)과 화재 예방 계획(FPP)을 수립하여, 조직이 비상사태에 어떻게 대응할지를 문서화하고, 사고 자체를 예방합니다.
- **컴플라이언스 서비스(Compliance Services):** 비상 계획 절차가 문서화되고 최신 상태로 유지되며, 관련 규제 기관의 요구 사항을 충족하도록 보장합니다.
- **교육 서비스(Training Services):** 직원들에게 대면 및 온라인 교육을 통해 다양한 안전 및 비상 상황에 대응하는 방법을 교육합니다. 교육 주제에는 화재 안전, 총기 난사 대응, 응급 처치, 테러 대응 등이 포함됩니다.

AI 기반 보안 계획 및 절차

AI는 조직의 보안을 혁신하고 있으며, 텍스트나 음성 명령을 통해 보안 시스템에서 중요한 정보를 추출할 수 있게 합니다.

자연어 처리(NLP) 및 자연어 이해(NLU)를 활용한 대화형 AI(Conversational AI)는

사후 조사 간소화, 정기 보안 점검, 고위험 이벤트 대비 준비 등을 보다 효율적으로 수행할 수 있게 합니다.

예를 들어, 중요한 인사가 본사를 방문하는 경우, 보안 팀은 단순히 “보안 수준을 높여라”라는 명령을 내리는 것만으로 특정 이벤트를 대비해 시스템에 미리 보안 프로토콜을 설정할 수 있습니다.

이러한 선제적 접근은 보안을 강화할 뿐 아니라, 조직의 안전 관리에 대한 조직의 헌신을 보여줌으로써 이해관계자의 신뢰를 높입니다.

88%의 조직이 비상 대응 계획을 가지고 있습니다[1]

계획에 대한 신뢰 수준:

매우 자신 있다: 9%
자신 있다: 39%
어느 정도 자신 있다: 35%
약간 자신 있다: 16%
자신 없다: 2%

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Partner Insight

클라우드 스토리지의 힘

비디오 관리 시스템(VMS)의 수명이 길어질수록 추가 저장 공간의 필요성은 지속적으로 증가합니다.비디오 보존 정책도 변화함에 따라, 데이터를 보호하기 위해 중복 백업 및 기타 보안 메커니즘을 도입해야 할 수도 있습니다.

온프레미스 스토리지를 추가하는 경우, 상당한 수준의 하드웨어 및 설치 비용이 발생할 수 있습니다. 대안으로 하이브리드 또는 완전 클라우드 스토리지를 선택할 수 있습니다.

이를 통해 추가 하드웨어를 구매하지 않고도 저장 용량을 유연하게 조정할 수 있으며, 데이터 보존 및 중복성을 강화하여, 규정 준수를 지원하고, 재해나 사이버 공격으로부터 데이터를 보호하기 위해 클라우드에 클라우드에 3중 백업 체계를 구축하여 데이터를 저장합니다.

최신 SaaS(서비스형 소프트웨어) 솔루션은 클라우드 스토리지 기능이 기본 내장되어 있습니다. 장치를 클라우드에 직접 연결할 수 있어, 추가 인프라 없이도 손쉽게 운영 및 확장이 가능합니다.

Genetec™ Security Center SaaS는 클라우드 네이티브 기능을 제공하며, 클라우드 카메라 직접 연결, 지속적인 클라우드 녹화 및 재생, 완전 호스팅 비디오 운영 기능을 지원합니다.

또한 하이브리드 옵션을 통해 엣지(Edge)에서 녹화 및 처리를 수행하거나 온프레미스 인프라와 연결하는 등 다양한 배포 옵션이 제공되어 조직의 고유한 요구사항에 맞게 구성할 수 있습니다.

[클라우드 스토리지는] 정책과 규정을 수하면서, 재해와 사이버 위협으로부터 데이터를 보호합니다.

파트너와 협력하여 비디오 관리 솔루션, 시스템 구조, 배포 방식을 최적화하세요. 비디오와 메타데이터를 로컬 또는 클라우드에 저장하는 다양한 방법이 있습니다.

하이브리드 접근 방식은 모든 현장에서의 유연성을 극대화할 수 있습니다. 통합 솔루션 파트너는 시스템과 운영을 최적화하여 물리적 보안 투자 효과를 극대화하도록 도와줄 수 있습니다.

Partner Insight

사이버 보안 위험으로부터 CPS 보호하기

스마트 센서부터 인공지능(AI) 카메라까지 확산된 강력한 IoT 시스템(사이버 물리 시스템, CPS)은 효율성을 제공하지만, 동시에 사이버 공격 표면을 크게 확장시킵니다.

새롭고 기존의 사이버 위협을 해결하는 유일한 방법은 효과적인 노출 관리입니다.

신경 프로세서, 고급 네트워킹, 맞춤형 메모리를 갖춘 물리적 보안 하드웨어는 '해커의 놀이터'를 만들어 냅니다.

신경 프로세서는 로컬에서 정교한 공격과 봇넷 참여를 가능하게 하고, 빠른 네트워킹은 데이터 탈취 및 악성코드 확산을 가속화합니다.

맞춤형 메모리는 민감한 데이터를 로컬에 저장하여 주요 공격 대상이 됩니다.

현실적인 영향에는 DDoS 공격 증가, 중요 정보 유출, 공급망 취약점, 물리적 보안 시스템 조작, 그리고 산업 스파이 활동이 포함됩니다.

현실적인 영향에는 DDoS 공격 증가, 중요 정보 유출, 공급망 취약점, 물리적 보안 시스템 조작, 그리고 산업 스파이 활동이 포함됩니다.

조직을 보호하기 위해서는 강력한 사이버 위생(cyber hygiene) 관리와 자동화된 대응 체계가 필요합니다.

물리적 보안 배포 환경의 복잡성과 다양성 때문에 자동화된 방식을 반드시 도입해야 합니다.

핵심 실천 방안으로는 다음이 있습니다:

- **펌웨어 자동 업데이트**
- **CPS 장치 분리를 위한 네트워크 세분화**
- **불필요한 서비스를 비활성화하여 장치 강화**
- **주기적인 비밀번호 변경**
- **제로 트러스트(Zero-Trust) 아키텍처 구현**
- **공급망 보안 평가**
- **CPS 보안에 대한 직원 교육**

강력한 CPS 장치의 등장은 기회이자 위험 입니다.

이러한 위험을 이해하고 강력한 보안 대책을 구현하는 것이, CPS의 효율성을 활용하면서 사이버 공격 노출을 최소화하는 핵심입니다.

준비는 선택이 아니라 필수입니다. Viakoo는 기업이 CPS 취약점을 발견하고 해결할 수 있도록 지원하며, Securitas Technology와 함께 AI 속도로 다가오는 물리적 보안 사이버 위협 대응을 선도하고 있습니다.

Partner Insight

INTELLICENE
UNIFYING SECURITY, ENABLING ACTION

확장 가능한 보안 시스템 (Security to Scale)

기업이 성장하고 새로운 지역으로 확장함에 따라, 성장의 기회를 맞이하는 동시에 점점 더 복잡한 보안 과제에도 직면하게 됩니다.

더 넓은 영역에서 보안을 관리하는 일은 복잡성과 부담이 커지고, 분산된 시스템, 데이터의 사일로화, 중앙 관리 부재로 인해 중요한 취약점이 노출될 위험이 커집니다.

확장 가능한 보안 시스템을 구축하는 것이 핵심입니다. 새로운 지점들이 각자 독립적으로 보안을 관리하기보다, 중앙화된 보안 관리 플랫폼을 통해 모든 지점의 보안 상태를 통합 및 상호 연계된 데이터 스트림으로 파악하고, 다양한 통합 기능을 무한히 확장할 수 있습니다.

보안 시스템을 하나의 중앙화된 플랫폼으로 통합하면, 보안 담당자는 위협을 식별·평가·예방할 수 있는 전체적인 가시성(holistic visibility)을 확보할 수 있습니다.

조직은 상호 연계된 보안 데이터 분석 가능한 사이트로 전환해 운영 효율성을 높일 수 있습니다.

이는 단순한 보안 관리에 그치지 않고, 고객 행동 패턴과 직원 생산성을 추적하여 리소스가 가장 효율적으로 사용되는 곳을 파악하고, 운영 효율성을 극대화하는 데 도움을 줍니다.

기업은 성장과 변화에 유연하게 대응할 수 있는 보안 포트폴리오가 필요합니다. 확장성과 유연성은 선택이 아닌 필수이며, 보안 투자 효과를 극대화하고 장기적인 성공을 보장하기 위한 핵심입니다. 당신의 보안 전략은 비즈니스의 성장에 맞추어 설계 되어 있습니까?

범죄 위험 인텔리전스의 미래

사람과 장소를 보호하기 위한 혁신적인 접근법

범죄의 흐름과 변동을 이해하는 것은 조직이 이해관계자를 보호하기 위해 매우 중요합니다. 특히 폭력이나 범죄 경향이 직원의 안전과 기업 운영에 직접적인 영향을 미칠 수 있는 지역에서는 더욱 그렇습니다.

범죄 위험 점수의 중요성

Pinkerton 범죄 위험 지수(PCI)와 같은 범죄 위험 점수는 정확하고 시의적절하며 정량화된 범죄 위험 측정 기준을 제공합니다.

위험 점수는 범죄 트렌드를 측정할 때의 불확실성을 제거하고, 조직이 전략적 보안 계획, 시설 위치 선정, 자원 배분, 보험 및 책임 관리, 이해관계자 안전, 평판 관리 등을 위한 데이터 기반의 결정을 내릴 수 있게 돕습 니다.

Pinkerton 범죄 위험 지수(PCI)는 범죄 데이터를 정밀하게 분석하기 위해 차세대 통계 기술과 혁신적인 방법론을 활용하는 범죄 위험 분석의 선두주자로 자리 잡고 있습니다.

PCI의 혁신과 기술

PCI는 범죄 위험 분석의 선두에 서 있는 지표로, 차세대 통계 기술과 혁신적인 방법을 활용하여 범죄 데이터의 세부적인 패턴을 포착합니다. 이 과정은 국가·지역·지방 단위의 법 집행 기관으로부터 데이터를 정밀하게 수집하고, 이를 교차 검증하여 보다 현실적인 범죄 상황을 파악하는 것에서 시작됩니다.

이후 불일치나 과소보고 문제를 해결하기 위해 데이터를 정제합니다. 예를 들어, 정확한 범죄율 산출을 위해서는 범죄 건수(분자)와 실제 인구 수 또는 유동 인구(분모)를 모두 반영해야 합니다. 이렇게 함으로써 단순 거주 인구뿐 아니라 관광객이나 통근자까지 포함한 실제 인구 기반의 범죄율을 산출할 수 있습니다.

또한 PCI는 범죄의 심각도에 가중치를 부여하여 형량, 피해 비용 등과 같은 요인을 고려하여, 중대한 범죄가 전체 위험 점수에 더 큰 영향을 미치도록 설계되어 있습니다.

마지막 단계에서는 예측 알고리즘이 정밀 검증 과정을 거쳐 정확도를 향상시킵니다.

고유한 과제와 맞춤형 솔루션

PCI가 다른 범죄 예측 솔루션과 다른 점은, 각 국가가 직면한 범죄 데이터 수집의 고유한 과제에 맞춘 접근 방식을 취한다는 것입니다. 현재 PCI는 미국, 캐나다, 멕시코, 브라질, 영국, 스웨덴, 호주에서 운영되고 있습니다.

멕시코에서는 과소보고가 심각한 문제이며, 호주의 범죄 데이터는 공개 시기와 분류 기준이 불일치해 일관성이 부족합니다. 또한 브라질의 보고서는 연도별 공백과 지역 간 차이가 존재합니다.

많은 범죄 및 위험 분석 도구가 공식 보고서에만 의존하는 반면, PCI는 피해자 조사, 사망 증명서, 지역 전문가 의견 등 공식 보고에서 누락된 정보를 추가적으로 분석해 보다 완전한 범죄 위험 평가를 제공합니다.

한계를 넘어

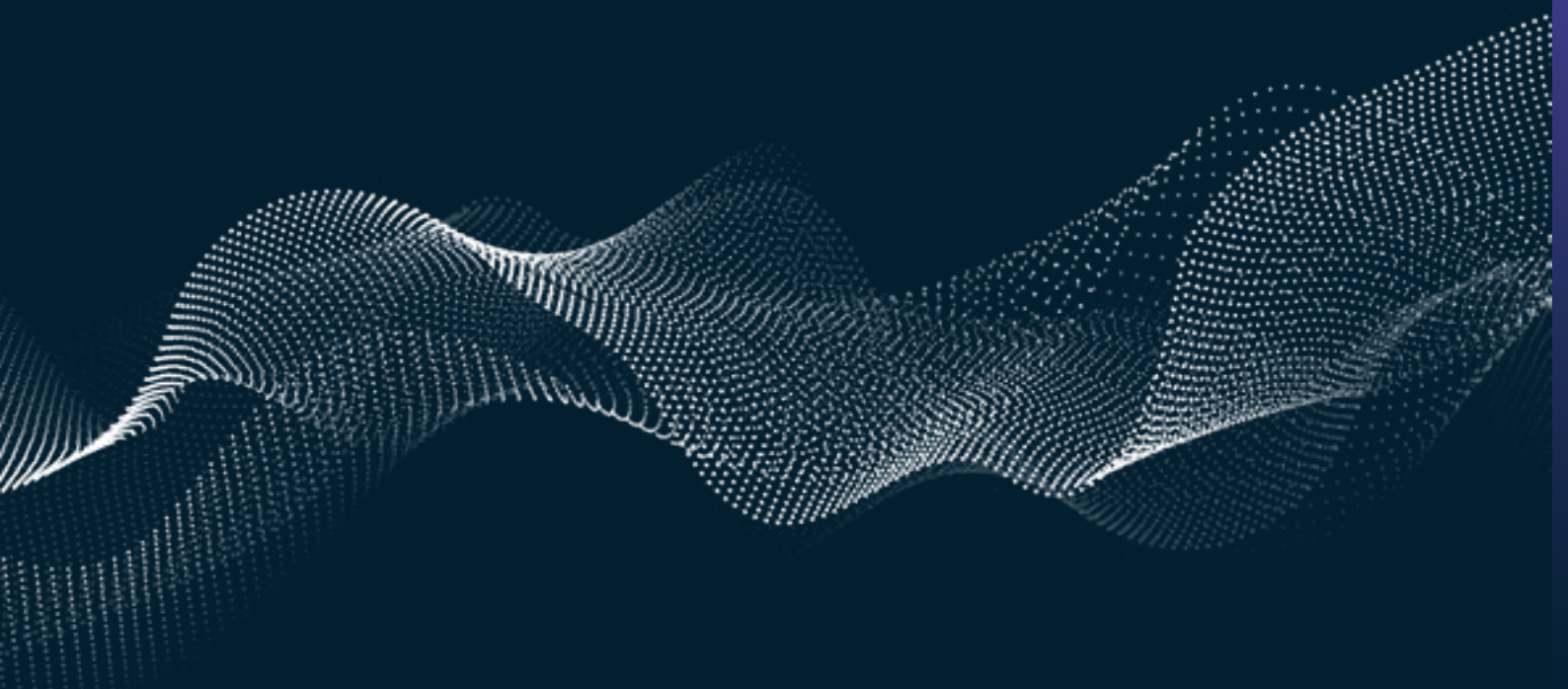
PCI는 매월 업데이트되며, 단순한 도구를 넘어 신적인 데이터 과학과 순련된 위험 관리 경험의 융합을 보여주는 도구로, 신뢰할 수 있고 미래 지향적 범죄 위험 관리의 도구로 자리잡고 있습니다.

Learn more at pinkerton.com

보안 전문가를 위한 실행 계획

> 오늘날처럼 불확실하고 변화가 심한 환경에서,
> 리테일 매장부터 캠퍼스, 기업 시설에 이르기까지
> 모든 환경의 보안을 강화하기 위해서는
> AI 기반 분석 기술, 비상 통신 시스템,
> 그리고 선제적 사고 대응 전략과 같은
> 첨단 기술이 필수적입니다.

Serdar Ince | Global VP, Technology Innovation
Securitas Technology



1 위험 완화를 위한 기술 검토

기존의 위험 완화 및 관리 방식을 평가하여 개선이 필요한 부분을 식별합니다. 직원과 고객의 안전, 그리고 전반적인 근무 환경을 향상시킬 수 있는 새로운 보안 기술, 교육 기회, 사고 대응 전략을 고려해야 합니다.

2 위험에 선제적으로 대응하는 방법 평가

현재의 위험 모니터링 프로세스와 기술을 검토하고, 정확성과 속도를 높일 수 있는 방안을 탐색합니다.
또한, 정보 분석 서비스에 투자하여 잠재적인 위협을 사전에 식별함으로써 새로운 위험이 발생할 때 조직이 정보를 기반으로 항상 대비할 수 있도록 합니다.

3 비상 대응 및 재해 복구 전략 업데이트

비상 대응 계획과 업무 연속성 계획을 지속적으로 검토하고 개선하세요. 기술과 커뮤니케이션 전략을 통합하여 대응 절차를 개선하고, 운영을 유지하며, 데이터를 보호하고, 위기 상황에서 직원의 안전 확보를 실현합니다.

4

보안의 새로운 흐름: 실시간 및 선제적 관리로의 전환

기업이 사건에 대응하는 방식에 큰 변화가 일어나고 있습니다. 이 변화는 자체 보안팀뿐 아니라 전문 보안 모니터링 제공업체를 통해서도 잘 드러납니다.

우리는 단순한 사후 검증의 시대를 넘어, AI기반 다중 데이터 분석을 통해 사고 대응의 속도를 높이고, 실시간 의사결정을 지원하는 지속적으로 학습하고 발전하는 지능형 보안 인프라로 이동하고 있습니다.

앞으로는 이러한 데이터가 다른 정보와 결합되어, 보안, 운영, 고객 및 직원 경험과 관련된 비즈니스 인텔리전스로 확장될 것입니다.

AI와 함께하는 보안 요원의 역할 강화

빠르게 변화하는 보안 환경에서, 효과적인 사고 대응의 핵심은 무엇이 진짜 중요한지 신속하게 파악하는 것입니다. 위협이 진화함에 따라, 대응 방식 또한 발전해야 합니다.

AI 기반 기술은 보안 요원의 업무 방식을 혁신적으로 변화시키고 있습니다. AI는 정확한 정보를 제공하여 요원들이 복잡한 문제 해결에 집중할 수 있도록 돕습니다. AI의 강점은 일관성과 집중력에 있습니다. 인간과 달리 AI는 피로하거나 집중을 잃지 않기 때문에 업무 분담에 있어 이상적인 가상 파트너(Virtual Partner) 역할을 합니다.

이러한 협력은 요원들이 가장 잘하는 일, 즉 세밀한 판단과 의사결정이 필요한 복잡한 문제 해결에 집중할 수 있도록 만들어 줍니다.

AI와 인간의 시너지로 얻는 이점

이 분야의 가장 주목할 만한 발전 중 하나는 영상의 이중 분석(Dual Analysis) 기술입니다. 엣지 분석(Edge Analytics)이 탑재된 카메라는 이제 대응이 필요한 활동을 자동으로 감감지하고, 분석 결과는 보안 관제 센터(SOC)에서 검토되어, 잠재적 위협이 정확히 식별되도록 합니다.

인간 에이전트가 오류를 발견할 때마다 AI 가상 에이전트는 학습을 통해 개선되며, 정상 활동과 의심스러운 활동을 구별하는 능력이 점 향상됩니다.

또한 가상 에이전트(Virtual Agent)는 경보 확인 과정에서 최종 사용자와의 상호작용을 처리하여 경보 대응의 효율성을 높이고 에이전트의 생산성을 강화합니다. 일상적인 업무를 자동화함으로써, AI는 보안 요원이 보다 중요한 업무에 집중할 수 있도록 돕습니다.

지능형 대응체계로 사고 대응 능력고도화

앞으로 AI 기반 사고 대응은 더욱 정교해질 것입니다. AI는 복잡한 상황을 더 높은 정확도로 해석할 수 있게 되며, “큰 짐을 든 사람이 있으면 경보를 울려라” 와 같은 자연어 명령을 통해 더 정확하고 세밀한 대응을 수행할 수 있습니다.

이는 물류창고 등 보안 요구가 다양한 환경에서 특히 유용할 것입니다.

하지만 조직이 AI를 도입할 때는, 개인정보 보호 및 윤리적 사용에 관한 법률과 규제를 준수하는 것이 필수적입니다. AI가 효과적이면서도 책임감 있게 활용되기 위해선 반드시 필요합니다.

궁극적으로, AI와 인간의 협력은 단순히 효율성을 높이는 것을 넘어, 각자의 강점을 발휘하며 정확하고 선제적인 보안 대응을 가능하게 합니다. AI의 강점을 활용함으로써 보안팀은 항상 한발 앞서 위협을 예방할 수 있습니다.

자동 감지(AI) 기술의 활용 현황[1]

조직별 활용 비율:

객체 인식
(Object Recognition):

이상 감지
(Anomaly Detection):

침입 및 배회 감지
(Intrusion and Loitering Detection):

차량 감지, 속도 및 방향 분석
(Vehicle Detection, Speed, and Direction):

인원 수 계산
(People Counting)

[1]2025년 2월부터 3월까지 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술에 대한 의사결정 권한을 가진 보안 전문가 575명을 대상으로 실시된 제3자 블라인드 설문조사.

Partner Insight

AI가 보안을 '반응형'에서 '예측형'으로 전환시키는 방법

보안 카메라가 촬영하는 영상의 대부분은 실제로 확인되지 않습니다. 그만큼 시간이 부족하기 때문입니다.

이 모든 영상을 실질적으로 활용하기 위해, 항상 작동하는 AI(Always-on AI)는 실시간으로 촬영과 동시에 영상을 분석하여 메타데이터를 생성하고, 사건을 식별하며, 대응을 자동화할 수 있습니다. AI는 대응 시간을 단축시켜, 사람들이 중요한 사건에 집중할 수 있도록 합니다.

AI는 현실적인 방법으로 '예측형 보안'을 실현합니다:

지정된 트리거(Trigger)에 따른 경보

- 차량이 하역장에 접근했나요?
- 근무시간 외에 복도에서 움직임이 감지되었나요?

불필요한 오경보 제거

AI는 날씨나 동물로 인한 잘못된 경보(오경보)를 거의 제거해, 불필요한 비용을 줄이고 경보의 신뢰성을 높입니다.

AI 기반 검색 효율화

AI 객체 인식(Object Recognition)과 태깅(Tagging)을 통해 "가방을 든 사람", "빨간 트럭"처럼 자연어 검색으로 사건을 쉽게 탐색할 수 있습니다.

차량 및 총기 식별 강화

차량 식별은 보안 사건 조사에서 핵심 요소입니다. Eagle Eye의 차량 번호판 인식 기술(License Plate Recognition) 은 의심 차량이 카메라에 포착되면 즉시 알림을 보냅니다.

AI는 영상을 유용한 정보로 전환해 즉각적인 사건 알림을 생성하고, 즉각적인 대응을 유도합니다.

또한 총기 감지 기술(Gun Detection Technology) 은 총이 발사되기 전에 무기를 식별할 수 있습니다.

무엇보다 중요한 점은, AI가 영상을 실시간으로 분석해 사건 발생 즉시 알람을 발생하고, 중요 사건을 조명(Spotlight) 한다는 것입니다.

Eagle Eye Cloud VMS는 지속적인 분석과 분류를 실현하며, 오픈 API(Open API)를 통해 다양한 기술 파트너와의 통합을 지원하여 특화된소프트웨어를 제공하는 프레임워크를 구축하고 있습니다.

Partner Insight

효과적인 경보 검증 (Alarm Verification) 전략

기존의 경보 모니터링은 “감지 후 통보(Detect and Notify)” 모델을 따릅니다.
즉, 모션 센서와 같은 감지 센서가 작동하면 중앙 관제 센터에 알림이 전송됩니다.

하지만 이러한 경보는 실제 위협을 확인하지 못해, 98%가 오경보(False Alarm) 로 이어집니다.

이에 따라 많은 지방자치단체는 오경보에 대한 벌금을 부과하거나, 경찰 출동 전 경보 검증 절차를 의무화하고 있습니다. 일부 지역에서는 실제 범죄가 진행 중인 확인된 경보에 대해서만 경찰이 우선 대응하도록 규정하고 있습니다.

다중 트립 감지(Multi-Trip Detection) 또는 강화된 통화 검증(Enhanced Call Verification) 과 같은 기술은 불확실성을 줄이지만, 실제 범죄 진행 여부를 완전히 확인하지는 못합니다.

가장 효과적인 검증 솔루션은 오디오 및 비디오 기반 검증(Audio & Video Verification) 입니다.
이를 통해 관제 요원이 실시간으로 현장의 소리나 영상을 확인할 수 있어, 대응 시간과 정확성이 향상됩니다.

> 일부 지역에서는 실제 범죄가 진행 중인 확인된 경보에 한해 우선적인 경찰 대응이 이루어집니다.

오디오(음성) 검증

- 시스템이 활성화된 상태에서 위협적인 소리를 감지합니다.
- 관제 요원이 실시간으로 청취하며 위협을 평가합니다.
- 천장부터 벽까지 공간 전체를 커버하여 조기 경보 감지를 가능하게 합니다

비디오(영상) 검증

- 경보 센서 또는 카메라 움직임 감지에 의해 트리거됩니다.
- 관제 요원이 경보 전·후 영상 클립 또는 실시간 영상 피드를 수신합니다.
- 범죄 진행 상황을 시각적으로 확인할 수 있습니다.

오디오와 비디오 검증의 통합은 경보 모니터링의 수준을 개선하여, 한 단계 끌어올립니다. 이 기술은 오경보를 줄이고 경찰 대응 효율성을 높이며, 오디오는 공간 전체에 대한 커버와 함께 조기 탐지를 제공하고, 비디오는 시각적 검증을 제공합니다.두 기술의 결합으로 보안 수준이 극대화되고, 빠르고 정확한 경찰 대응이 가능해져 오늘날 가장 신뢰받는 알람 모니터링의 업계 표준으로 자리 잡고 있습니다.

Partner Insight

BOSCH
Invented for life

선제적 대응과 자동화된 의사결정을 가능하게 하는 AI

AI는 영상 보안(Video Security)의 역할을 재정의하고 있습니다. 시각적 지능(Visual Intelligence)을 통해 사용자들이 영상 속에서 의미 있는 정보를 찾아내고, 패턴을 인식하며, 다음에 일어날 일을 예측하도록 돕습니다.

정확하고 빠른 감지는 위협이 문제로 발전하기 전에 조기에 식별하고 대응할 수 있게 합니다.

AI 기반 솔루션은 경계 침입(Perimeter Breach), 무기 노출(Brandished Guns), 보호 장비 미착용(Missing PPE) 등 다양한 보안 이상 징후를 신속하고 안정적으로 감지합니다.

AI 솔루션은 또한 여러 카메라에서 수집한 데이터를 통합·시각화하여 보안, 안전, 운영 관련 인사이트를 제공합니다.

이 데이터를 활용하면 트렌드 분석(Trend Analysis)이 가능해지고, 보안 및 안전에 영향을 미치는 패턴을 이해함으로써 사건 발생 가능성이나 영향력을 최소화하는 정보 기반 의사결정을 내릴 수 있습니다.

AI는 주의가 필요한 시점을 자동으로 인식하여, 사건이 발생한 후 대응하는 것이 아니라 선제적으로 조치를 취할 수 있도록 돕습니다.AI의 기능은 곧 객체 인식(Object Detection)을 넘어 장면의 맥락(Scene Understanding)을 깊이 있게 분석하는 수준으로 확장될 것입니다.
이는 복잡한 환경을 해석하고, 상황에 대한 통찰을 제공하며, 특정 객체나 행동으로 사전 학습되지 않아도 이미지를 분석할 수 있습니다.

또한 조직의 프로세스와 연동되어,
위험 완화 조치 제안 및 실시간 경보까지 가능하게 하며 사용자에게 더 큰 가치를 제공합니다.

AI는 단순한 객체 인식을 넘어, 복잡한 상황을 이해하고 예측하는 단계로 진화하고 있습니다.

지속적인 개선을 위한 데이터 분석

보안 운영의 영역에서 다양한 데이터 소스를 모니터링할 수 있는 능력은 보안과 비즈니스 인텔리전스 모두를 강화하는 새로운 서비스의 기반이 되어 산업 전반의 판도를 바꾸고 있습니다.

더 스마트한 SOC 운영 도구

보안관제센터(SOC, Security Operations Center)는 단순한 시스템 모니터링을 넘어 보다 정교한 보안 및 운영 관리 접근 방식을 가능하게 하며, 그 역량을 계속 확장하고 있습니다.

이미 다양한 부가 서비스가 도입되어 있으며, 예를 들어 자산 추적(Asset Tracking) 기능은 조직의 차량 및 고가 자산을 실시간으로 모니터링할 수 있게 합니다.

차량의 위치 정보를 실시간으로 확인해 예기치 못한 지연이나 안전사고가 발생할 경우 물류 관리자에게 즉시 알림을 보냄으로써 운영의 원활함과 보안 수준을 높일 수 있습니다.

이러한 데이터 통합은 현대 보안 시스템이 비즈니스 운영을 효율적으로 지원할 수 있는 잠재력을 보여줍니다.

AI 또한 관제센터 운영을 혁신하고 있습니다. AI 기반 가상 에이전트(Virtual Agent)는 여러 카메라를 순회하며 카메라의 설치 상태와 현재 상태를 비교해 초점이 맞지 않거나 위치가 어긋난 카메라를 자동으로 식별합니다.

이러한 선제적(Proactive) 접근 방식은 감시 시스템이 항상 최적의 상태로 작동하도록 보장합니다.

또한 AI는 원격 유지보수 작업도 지원합니다. 배터리 상태, 감지기 및 출입문 센서 상태를 점검하고, 영상이 올바르게 저장되었는지를 확인합니다. 이러한 기능은 다운타임(downtime)을 줄이고 보안 시스템의 신뢰성과 안정성을 높여줍니다.

예측형 플랫폼으로 전환 진행 중

AI의 가장 큰 영향력 중 하나는 이벤트 데이터를 분석하여 패턴을 식별하는 능력입니다. 이를 통해 조직은 유사한 상황에 더 잘 대비할 수 있습니다.

많은 보안관제센터(SOC, Security Operations Centers), 그 중에서도 특히 Securitas Technology의 SOC는 알람 이벤트 데이터를 축적한 데이터 레이크(Data Lake) 를 보유하고 있습니다.
이 데이터는 시간대, 요일, 계절적 추세 등 다양한 패턴으로 분석될 수 있습니다. 조직은 이러한 정보를 다른 데이터 소스(운영 데이터, 재무 데이터, 건물 자동화 시스템 데이터, 사이버 위협 모니터링 등)와 결합해 전체적인 위험 환경에 대한 더 풍부한 인사이트를 얻을 수 있습니다.

이 데이터를 기반으로 한 예측형 플랫폼(Predictive Platform) 이 이미 등장하기 시작했으며, 향후 몇 년 안에 예측 분석(Predictive Analysis) 이 실질적인 현실이 될 전망입니다.

새로운 형태의 지능형 분석(Intelligence) 은 이벤트 간의 연관성을 파악하여 사고의 원인을 이해하고 유사한 조건이 다시 발생할 가능성을 예측할 수 있도록 도와줄 것입니다. 이러한 사전 인식(Foreknowledge) 은 기업이 선제적인 대응 조치를 취할 수 있게 하여 위험을 줄이고 전반적인 보안을 강화합니다.

결론적으로, 지속적 개선을 위한 데이터 분석은 단순히 사건에 대응하는 것을 넘어, 예측 기반의 전략적 보안 모델로 발전하고 있습니다. AI와 데이터 분석이 발전함에 따라 보안 운영은 더욱 지능적(Intelligent)이고, 민첩(Responsive)하며, 그리고 효율적(Effective) 으로 진화할 것입니다.

이러한 데이터의 힘을 활용함으로써, 조직은 앞으로 다가올 어떤 위험에도 대비할 수 있는 준비태세를 갖출 수 있습니다.

> “AI는 단순히 보안 성과를 향상시키는 데 그치지 않습니다. 수작업을 줄여 총소유비용(TCO) 을 낮추고, 조직이 기존 자원을 더 효율적으로 활용할 수 있게 합니다. 예측형 위협 분석에서 자동화된 대응에 이르기까지, AI는 우리의 모든 보안 솔루션에 영향을 미치며 고객이 변화하는 위험에 한발 앞서 대응하고 운영 효율성을 극대화하도록 돕습니다.”
>
> Software House

Partner Insight

MOTOROLA SOLUTIONS

연결형 보안의 잠재력을 실현하다

보안의 진화는 수많은 개별 시스템에서 완전히 연결된 생태계로의 패러다임 전환을 요구합니다.

사용자에게 이는 단순한 장치 통합이 아니라, 실시간으로 위협을 예측하고 완화할 수 있는 지능적이고 유연한 보안 프레임워크를 설계하는 것을 의미합니다.

이 비전의 핵심은 개방적이고 상호운용 가능한 플랫폼(Open and Interoperable Platforms) 입니다. ONVIF와 같은 표준을 채택함으로써 벤더 간의 장벽을 허물고, 최고의 기술들이 융합된 동적 생태계(Dynamic Ecosystem) 를 구축할 수 있습니다.

이를 통해 각 조직은 자신의 요구에 맞춘 맞춤형 보안 솔루션을 설계할 수 있으며, 혁신과 회복탄력성을 동시에 강화할 수 있습니다.

또한 데이터 기반 인텔리전스(Data-Driven Intelligence)가 핵심입니다.

중앙집중형 분석과 AI의 힘을 활용해 원시 데이터를 실행 가능한 인사이트로 전환해야 합니다.

이를 통해 조직은 위협을 선제적으로 감지하고, 자동 대응(Auto-Response) 및 예측형 보안 모델링(Predictive Modeling) 을 통해 보안을 단순한 '반응적(Reactive)' 단계에서 '사전적(Preemptive)' 단계로 끌어올릴 수 있습니다.

서로 연결된 세상에서 사이버 보안은 전략적 필수 요소(Strategic Imperative) 입니다. 기기 인증부터 네트워크 분할까지, 모든 단계에 강력한 보안 프로토콜을 내재화해야 합니다.

클라우드 기반 플랫폼은 원격 관리, 실시간 협업, 데이터의 원활한 공유를 가능하게 하여 조직이 새로운 위협에 신속하게 대응하고 운영 효율성을 최적화할 수 있도록 지원합니다.

클라우드 기반 플랫폼은 원격 관리, 실시간 협업, 데이터의 원활한 공유를 가능하게 하여 조직이 새로운 위협에 신속하게 대응하고운영 효율성을 최적화할 수 있도록 지원합니다.

진화하는 사이버 위협으로부터 생태계의 무결성을 보호하기 위해서는 예방적이고 다층적인 접근 방식(Proactive and Layered Approach) 이 필수적입니다.

클라우드 기술의 전략적 도입은 그 어느 때보다 확장성(Scalability) 과 접근성(Accessibility) 을 극대화합니다. 이러한 기술은 조직이 민첩하게 위협에 대응하고 운영 효율성을 높이는 데 기여합니다. 결국, 진정으로 연결된 보안 생태계는 인간 중심적(Human-Centric) 이어야 합니다.

직관적인 사용자 인터페이스와 체계적인 교육을 통해 보안 전문가들이 기술의 잠재력을 최대한 활용할 수 있도록 해야 합니다. 인간의 전문성과 기술 혁신이 융합될 때, 새로운 보안의 시대가 열릴 것입니다.

이러한 전략적 방향성을 수용함으로써 우리는 자산을 보호할 뿐만 아니라 운영 효율성을 향상시키고, 선제적 보안 문화(Proactive Security Culture) 를 구축할 수 있습니다.

Partner Insight

MARCH networks
A Delta Group Company

멀티 사이트 비디오 관리 시스템(VMS)

여러 위치에서 비디오 감시를 관리하는 것은 매우 복잡한 과제입니다.

오늘날의 기업은 비디오 관리를 중앙화하고, 시스템의 안정성을 유지하며, 보안과 운영 효율성을 높이는 실행 가능한 인사이트를 제공하는 시스템이 필요합니다.

March Networks의 업계 선도적인 엔터프라이즈 비디오 관리 솔루션은 복잡한 다중배포를 간소화하고, 확장 가능한 관리 환경을 제공합니다.

강력한 비디오 관리 시스템(VMS) 은 기업이 모든 지점을 단일 인터페이스에서 모니터링할 수 있도록 하여 데스크톱, 웹, 또는 모바일을 통해 중앙에서 제어할 수 있습니다.

March Networks Command Enterprise Software (CES) 를 통해 조직은 수천 대의 카메라, 녹화 장치, 비디오 채널을 관리하며, 실시간 시스템 상태 모니터링, 사용자 활동 추적, 맞춤형 보안 화면 구성을 통해 보안팀이 적극적이고 신속하게 대응할 수 있습니다.

Command Enterprise Cloud는 중앙 집중식 비디오 저장소, 안전한 원격 접속, 무제한 확장성을 제공하여 현장 인프라를 부담 없이 운영할 수 있게 합니다.

또한, AI 기반 분석(AI-driven Analytics) 은 비디오 데이터를 트랜잭션 데이터 및 IoT 장치와 통합함으로써 기업이 필요한 영상을 90% 더 빠르게 찾을 수 있도록 지원합니다.

March Networks의 Searchlight Cloud는 사기, 도난, 법적 리스크, 운영 비효율성을 감지하고 실시간 경보와 대시보드를 통해 기업 전체와 개별 지점 수준의 인텔리전스를 제공합니다.

포괄적이고 유연하며
확장 가능한 엔터프라이즈 VMS를 활용함으로써 기업은 자산을 보호하고, 운영을 간소화하며, 모든 지점에서 더 현명한 의사결정을 내릴 수 있습니다.

이러한 이유로, 세계 최대 규모의 복잡한 은행을 포함해 총 1,500개 이상의 금융기관이 March Networks의 엔터프라이즈 비디오 관리 솔루션을 신뢰하고 있습니다.

AI 기반 분석은 트랜잭션 데이터와 IoT 장치를 비디오와 통합하여 기업이 필요한 영상을 90% 더 빠르게 찾을 수 있도록 지원합니다.

Partner Insight

IDIS One Solution. One Company.

고속·고화질 영상의 잠재력: AI와 클라우드 기술이 만드는 감시 혁신

기업들이 점점 더 클라우드 기반 솔루션을 채택함에 따라, 고속·고화질 영상 감시는 그 어느 때보다 중요해졌습니다.

클라우드는 확장성, 원격 접근, 중앙 집중식 관리를 가능하게 하지만, 품질을 유지하면서도 우수한 영상과 성능 을 확보하는 것은 쉽지 않은 과제입니다.

IDIS(아이디스)는 이러한 과제를 해결하기 위해 고속 스트리밍과 탁월한 영상 품질을 동시에 제공하는 고급 기술 전략을 결합했습니다.

이 솔루션의 핵심은 IDIS Intelligent Codec(지능형 코덱) 으로, 영상의 선명도를 유지하면서도 대역폭과 저장 공간 요구를 줄이는 기술입니다.

기존의 압축 방식과 달리, IDIS Intelligent Codec은 최대 50% 더 높은 효율성을 제공하여 기업이 고화질 영상을 더 빠르게 스트리밍하고 고비용 인프라 업그레이드 없이 클라우드에 더 많은 영상을 저장할 수 있도록 합니다. 이를 통해 언제 어디서나, 다양한 네트워크 환경에서도 실시간 영상과 녹화 영상을 원활하게 확인할 수 있습니다.

AI 역시 영상과 음성 처리의 품질 향상에 중요한 역할을 합니다. AI는 색상, 해상도, 선명도를 정교하게 조정하여 최소한의 데이터로도 고품질 영상을 구현합니다.

또한 영상 분석에서는 메타 프로세싱 프레임(Meta-Processing Frames) 을 통해 감지 정확도를 높이고, 음성 분석에서는 사람의 음성을 분리하고 주변 소리를 증폭하여 역노이즈 캔슬링(reverse noise canceling) 과 같은 기능을 가능하게 합니다. 이러한 AI 기반 향상 기능은 보안 시스템을 더 빠르고 정밀하게 작동하도록 만듭니다.

IDIS는 AI및 영상 압축 기술을 결합한 클라우드 기반 솔루션을 통해, 기업들이 효율적이고 확장 가능한 고품질 영상 감시 체계를 다양한 산업 전반에 걸쳐 구축할 수 있도록 지원합니다.

Securitas

보안요원의 역할 강화:

교육과 기술이 만들어내는 변화

감시 카메라, 출입 리더기, 온도 모니터링 태그, IoT 장치 등 오늘날의 비즈니스 환경은 보안 및 운영 데이터를 실시간으로 처리하는 연결형 센서들로 가득합니다.

하지만, 현장에는 또 다른 강력한 센서가 있습니다. 그것은 바로 보안요원(Security Officer) 입니다. 전 세계 수천 개의 사업장에서 보안요원은 일상적인 비즈니스 운영의 핵심적인 역할을 수행합니다.

환경의 미묘한 변화를 관찰하고, 실시간으로 결정을 내리며, 보안 사고를 예방하고 대응하고 해결합니다. 기술과 자동화가 발전함에도 불구하고 보안요원의 가치는 오히려 높아지고 있습니다.

그들의 역할이 점점 더 비즈니스 보안의 핵심 요소가 됨에 따라 보안요원에 대한 지속적인 투자와 그들의 역할에 대한 지원은 그 어느 때보다 중요합니다.

오늘날 Securitas에서 이러한 변화가 어떻게 이루어지고 있는지, 세 가지 예시로 살펴보겠습니다.

1. 경비에서 정보 기반 보호로의 전환 (Intelligence-Led Protection)

실시간 위험 인텔리전스 플랫폼을 도입하는 기업이 늘고 있지만, 경보(Alert)를 실제 행동으로 전환하는 데 어려움을 겪고 있습니다.

Securitas는 올바른 교육을 받은 보안요원이 이 격차를 메울 수 있다고 믿습니다. Securitas는 보안요원이 정보 분석의 기본 역량(Intelligence Fundamentals) 을 습득할 수 있도록 시범 교육 프로그램(Pilot Program) 을 개발했습니다.

이 프로그램은 정보 분석가로서의 핵심 기술을 교육하며, 다양한 정보 수집원(예: 지역 응급 서비스)과 협력하고, 조직에 중요한 정보를 식별하고 분석하는 방법을 배웁니다.

또한, 변화하는 위협 환경 속에서 정보 분석을 활용해 선제적으로 대응하는 능력(Proactive Capability) 을 강화합니다..

무엇보다도, 보안요원은 현장에서의 정보 분석을 현장 의사결정에 통합하는 방법을 배우며, 조직이 더 빠르게 대응하고, 지역 수준에서 병목현상을 줄일 수 있도록 돕습니다.

자세히 보기: securitas.com

시큐리타스의 관점: 보안요원의 역할 재정의 데이터 센터 보안 전문 역량 강화

데이터 센터 보안 전문 역량 강화

시큐리타스는 세계에서 가장 중요하고 빠르게 성장하는 산업 중 하나인 데이터 센터(Data Center)의 복잡한 요구를 충족하기 위해 10,000명 이상의 보안요원을 대상으로 한 전문 교육 프로그램을 운영하고 있습니다.

이 프로그램은 2024년에 시작되어 HISPI (Holistic Information Security Practitioner Institute)의 인증을 받았으며, 보안요원들은 공인 데이터 센터 보안 전문가(Certified Data Center Security Professional) 로서 고위험·고보안 환경에서 요구되는 특화된 역량을 갖추게 됩니다.

기존의 '획일적인(one-size-fits-all)' 경비 방식은 데이터 센터와 같은 고위험·고보안 환경에서는 더 이상 충분하지 않습니다. 따라서 이러한 고급 지식과 전문화는보안요원이 데이터 센터의 보안 수준을 향상시키고 복원력을 강화하는 핵심 자원이 되도록 합니다.

보안요원 배치 및 이동 경로 최적화

보안요원이 전략적인 역할을 수행하도록 훈련하는 동시에, 기술은 배치 효율성과 운영 최적화에 중요한 역할을 합니다.

시큐리타스는 여러 유럽 국가에서AI 모델을 도입하여 보안요원 배치를 최적화 하고 있습니다. 출퇴근 시간, 기술 적합도, 장기 인력 수요 예측 등을 고려해 최적의 배치를 가능하게 합니다. 예를 들어, 베를린 대도시 지역에서는 최적화된 경로 설정을 통해 일일 출퇴근 거리를 44%까지 줄일 수 있는 잠재력이 있습니다.

또한 AI는 보안 근무지 최적화에도 활용되고 있으며, 독일에서는 이미 평균 운행 시간을 10% 단축시켜 운영 효율성 향상과 비용 절감을 실현했습니다.

이러한 변화들은 보안요원의 업무 효과를 배가시키고, 더 빠른 지원, 더 높은 효율성, 그리고 고객 만족도 향상으로 이어지고 있습니다.

보안요원의 역할 재정의

이 모든 사례들은 우리가 보안(Security) 과 사람(People)을 어떻게 바라보는지에 대한 근본적인 변화를 보여줍니다.

가장 효과적인 보안 전략은 기술만으로 완성되지 않습니다. 그 중심에는 훈련되고, 신뢰받으며, 연결된 사람들이 있습니다. 이들은 조직의 보안 생태계에 자연스럽게 녹아들어 안정적인 운영을 가능하게 합니다.

산업이 계속 진화하는 가운데, 시큐리타스는 언제나 '사람 중심의 보안' 을 핵심 가치로 삼고 있습니다. 고급 교육, 전문화된 기술, 그리고 AI를 통해 우리는 보안요원들이 미래의 변화에 대비할 수 있도록 지원하고, 그들이 보호하는 조직의 복그들이 보호하는 조직의 회복탄력성(Resilience)을 강화하고 있습니다.

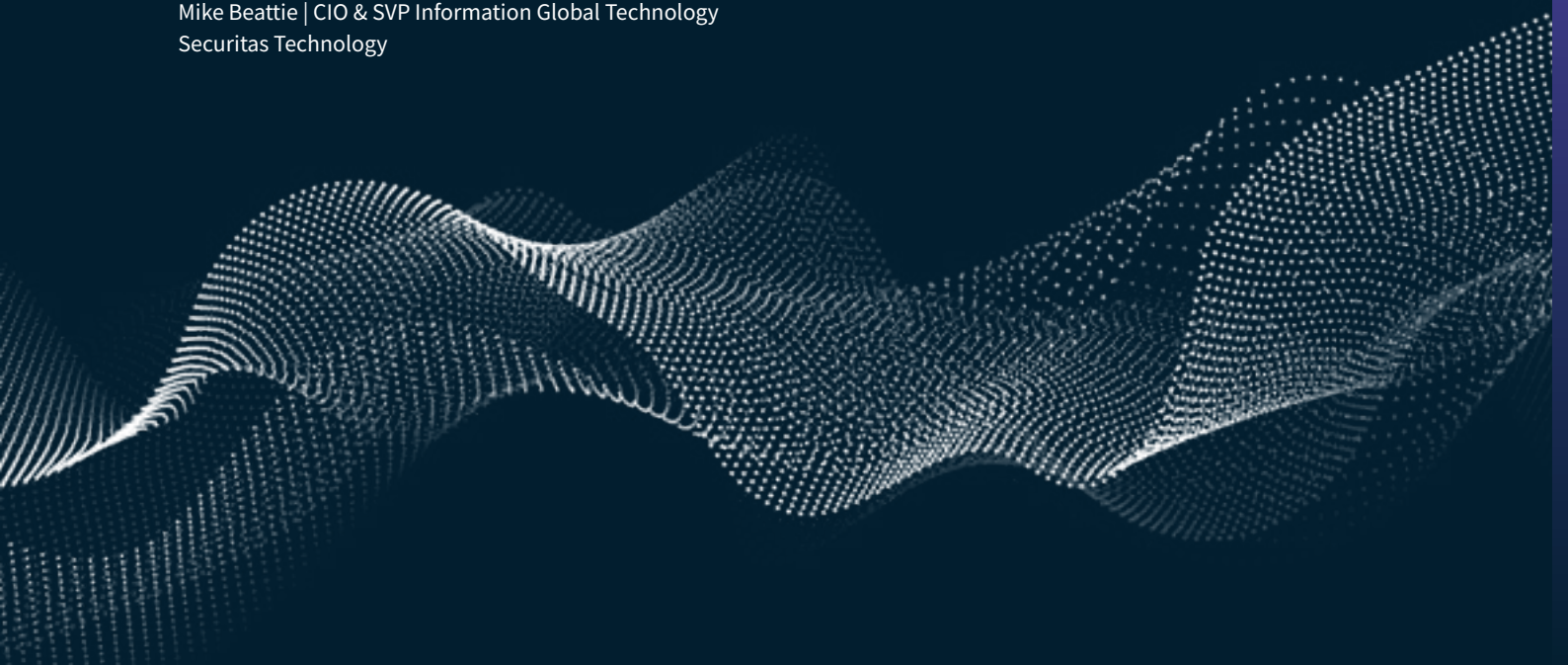
보안 전문가를 위한 실행 계획

"보안의 미래는 실시간·선제적 관리 체계로 빠르게 전환되고 있으며, 인공지능(AI), 데이터 통합, 그리고 네트워크 기술 발전에 의해 주도되고 있습니다.

AI를 활용해 사람의 역량을 보완함으로써, 조직은 사건 대응 속도를 높이고, 운영 효율성을 강화하며, 위협을 더 정확하게 예측할 수 있습니다.

하지만 이러한 강력한 기술을 도입할수록, 조직은 네트워크 보안, 개인정보 보호, 그리고 AI의 책임 있는 활용을 위한 규정 및 표준을 철저히 준수하는 것이 더욱 중요해집니다."

Mike Beattie | CIO & SVP Information Global Technology
Securitas Technology



1 보안 사고 대응 절차 검토

조직 전반에서 사건이 어떻게 모니터링되고 관리되는지 종합적으로 평가합니다. 이는 경보 대응 절차부터 일상적인 보안 업무까지 포함됩니다.

또한, 보안 서비스 제공업체의 기술 로드맵을 이해하고 자동화, 요원 지원, 데이터 분석이 가능한 정보 생태계의 구축을 검토합니다.

2 선제적 보안 기술에 대한 투자 우선순위 설정

예산 내에서 최신 기술과 데이터 통합 솔루션을 구현하기 위한 자원을 배분합니다. 이를 통해 위협 감지, 사고 대응, 분석 능력을 선제적으로 강화할 수 있습니다.
또한, AI 기반 자동화 및 원격 서비스를 도입해 보안 운영을 미래지향적이고 민첩하게 대응하는 체계로 전환합니다.

3 AI통합 사고 대응 절차에

내부 이해관계자들과 협력하여 AI를 사고 대응 프로토콜에 통합하기 위한 전략적 계획을 수립합니다.

기존 절차를 AI 솔루션으로 강화하는 데 집중하며, 이 과정에서 법률, 규제, 윤리 기준 준수를 철저히 보장합니다.

5

조직의 영향력과 가치를 창출하는 보안 시스템

보안의 중요성은 오래전부터 잘 알려져 왔습니다. 이는 개인과 조직 모두의 안전과 복지를 보장하는 인간의 기본적인 필수 요소입니다.

보안 시스템은 사람과 자산을 보호하고, 생명을 위협하는 재난을 예방함으로써 그 가치를 꾸준히 증명해 왔습니다.

보안 및 손실 방지 전문가들은 인간의 안정적인 삶을 유지하고 평온함을 제공하는 필수적인 역할을 수행하고 있습니다.

이제 보안 시스템은 그 이상을 실현할 수 있는 잠재력을 가지고 있습니다.

보안 시스템은 방대한 양의 데이터를 생성하여 조직이 운영 효율성을 높이고, 의사결정을 개선하며, 혁신을 추진할 수 있는 새로운 기회를 제공합니다.

이는 기업이 보안 기술을 통해 단순한 보호 수단을 넘어 전체적인 성공에 기여하는 전략적 자산으로 전환할 수 있음을 보여주는 새로운 관점입니다.

비즈니스 최적화에 기여하는 보안 데이터

우리는 데이터 중심의 시대에 살고 있습니다. 조직은 모든 활동에서 분석의 필요성을 인식하고 있으며, 보안 분야도 예외가 아닙니다. Securitas는 고객과 협력하여 여러 보안 시스템에서 데이터를 통합하여 보안 활동의 패턴을 보다 정밀하게 분석하고, 더 넓은 비즈니스 개선 노력에 도움이 되는 통찰을 도출할 수 있도록 지원하고 있습니다.

고객 및 직원 경험 개선은 보안 기술의 상위 5대 핵심 요인 중 하나입니다.[1]

데이터 통합을 통한 인사이트 확보

많은 조직들이 여러 보안 시스템의 데이터를 결합하여 보안 시스템 간의 상호작용을 종합적으로 이해하려는 수요가 증가하고 있습니다.

이러한 접근은 보안 사고가 언제, 왜 발생하는지 이해하는 데 도움이 되는 데이터 트렌드를 식별하는 것에 초점을 맞추고 있습니다.

예를 들어, 보안 관리자는 출입통제 로그와 영상 감시 시스템 데이터를 통합하여 직원의 안전과 관련된 중요한 인사이트를 도출할 수 있습니다.

AI의 도움을 통해 이러한 데이터를 분석하면, 폭력 사건이 발생하기 쉬운 시간과 장소를 정확히 파악할 수 있습니다.

또한, 조직은 내부 시스템(운영, 재무 등)의 데이터뿐만 아니라 사이버 위협 및 리스크 인텔리전스 데이터와도 보안 데이터를 통합하여, 조직의 위험과 성과를 보다 거시적으로 파악할 수 있는 시각을 구축하고 있습니다.

AI를 활용한 이벤트 상관관계 분석은 이러한 다양한 데이터 소스 간의 관계를 파악함으로써, 보안 위협뿐 아니라 비즈니스 전반에 걸친 새로운 알림과 인사이트를 제공할 수 있습니다.



[1]2025년 2월부터 3월까지 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술에 대한 의사결정 권한을 가진 보안 전문가 575명을 대상으로 실시된 제3자 블라인드 설문조사.

AI와 사이버보안 규제 환경의 변화하는 규제환경

보안 전문가와 IT, 법무, 컴플라이언스 담당자가 주목해야할 두 가지 주요 규제 트렌드가 있습니다.

2024년 8월 제정된 EU AI 법(EU AI Act)은 책임 있는 AI 사용을 위한 기준을 마련했으며, 일부 적용 사례에 대해서는 2025년 2월부터 준수 의무가 시작됩니다.
조직은 자사의 AI 사용이 해당 법에 따라 어떻게 분류되는지 파악하고 그 요구 사항을 준수해야 합니다.
미국에서는 콜로라도 AI 법(Colorado AI Act)이 미국 최초의 일반 AI 법안으로 제정되었고, 뉴욕, 플로리다, 유타주 등은 보다 특화된 법안을 마련하고 있습니다.

글로벌 차원에서도 호주, 캐나다, 영국 등이 유사한 입법을 추진 중입니다. 또한 사이버보안 규제도 진화하고 있습니다.

EU의 네트워크 및 정보보안 지침(NIS2 Directive)은 2024년 10월부터 시행되며, 물리적 보안 시스템을 포함한 핵심 산업에 대한 사이버보안 기준 강화를 의무화하고 있습니다.미국의 경우, 연방 차원에서는 금융, 기간산업 등 특정 산업을 대상으로 한 규제가 있으며, 주별 개인정보 보호법이 영상 데이터 보호 등 보안 조치에 영향을 미치고 있습니다.

고객 경험 향상

고객의 보안 데이터를 통해 상호작용과 선호도를 이해함으로써, 기업은 맞춤형 서비스를 제공하고 환경을 개선하여 고객 경험을 향상시킬 수 있습니다.
특히 리테일 매장에서는 고객 행동에 대한 인사이트를 통해 매장 내 혼잡 구역을 파악하고 상품 진열을 최적화할 수 있습니다.

이러한 전략은 매출 증가에 직접적인 영향을 미치는 요인이 될 수 있습니다.

호텔 산업에서도 사전에 수집된 고객 선호도(객실 온도, 조명 설정 등)를 기반으로 체크인 시 자동으로 환경을 조정하는 맞춤형 서비스를 제공할 수 있습니다.

이처럼 데이터 기반 인사이트에 따른 조정은 고객 만족도와 충성도를 높이는 동시에 성공적인 운영을 지원하는 효과적인 방법입니다.

업무 환경 최적화

기업 보안 시스템은 건물 내 활동 데이터를 지속적으로 수집하여, 출입통제 기록이나 경보 해제 등 각종 상호작용을 통해 유용한 인사이트를 제공합니다.
사무 환경에서는 출입통제 및 영상 데이터 분석을 통해 직원의 이동 패턴과 공간 활용도를 파악하고,
이를 기반으로 회의실 예약, 조명 및 온도 일정 조정, 사무실 레이아웃 재설계 등을 통해 효율성과 직원 만족도를 향상시킬 수 있습니다.

하지만 이러한 데이터 분석에는 시간과 집중력이 요구되며, 보안 및 시설 관리자는 종종 다른 우선순위로 인해 분석에 집중하기 어렵습니다.
AI 기술은 방대한 데이터 세트를 효율적으로 처리하고실행 가능한 인사이트를 도출하여 해당 과정을 단순화할 수 있습니다.

또한, 환경 센서를 보안 시스템에 통합하면 공기 질 변화나 유해 물질(예: 대마 성분 THC) 감지와 같은 추가적인 workplace 안전 모니터링이 가능합니다.
학교나 사무실에서는 이를 통해 무단 흡연이나 위험 화학물질의 존재를 실시간으로 감지 및 경고할 수 있습니다.

Partner Insight

현대 보안 산업에서의 책임 있는 AI 활용

AI가 보안 산업의 미래를 계속해서 변화시키는 가운데, 기업은 AI의 위험성과 이점을 모두 명확히 이해하는 것이 중요합니다.
보안 서비스 제공업체들은 오랜 기간 AI 솔루션에 대한 경험을 바탕으로 AI 관련 과제를 해결하는 데 있어 한발 앞서 있습니다.

그러나 AI의 활용은 법적 준수에만 국한되지 않으며, 투명성과 윤리적 고려가 반드시 수반되어야 합니다. 경제협력개발기구(OECD)가 제시한 인간 중심의 AI 프레임워크는 고객이 AI의 작동 방식과 한계를 이해하도록 하는 것이 신뢰 구축의 핵심임을 강조합니다. 이를 통해 기업은 파트너와 고객과의 신뢰를 강화할 수 있습니다.

보안 분야에서 AI의 주요 목표는 업무 자동화와 실행 가능한 인사이트 제공입니다.
AI 기반 자동화는 효율성을 높이지만, 동시에 AI 오류로 인한 잠재적 위험을 평가하는 것이 중요합니다.

책임 있는 AI활용은 윤리적 설계와 신중한 사용을 모두 필요로 합니다.

AI의 기능과 한계를 투명하게 공개함으로써, 기업은 보다 정확한 의사결정과 효과적인 리스크 관리를 수행할 수 있습니다. 이는 특히 제조업이나 주요 기반 시설과 같은 핵심 산업 분야에서 더욱 중요합니다.

또한, AI 시스템은 편향성과 한계에 대해 평가되어야 하며, 다양한 조건에서 데이터를 분석할 때 그 정확성과 공정성을 검증해야 합니다.생성형 AI와 같은 신기술이 등장함에 따라, 실제 환경에서의 강화된 테스트를 통해 그 영향을 면밀히 이해해야 합니다.

결국, 책임 있는 AI 활용은 윤리적 설계와 신중한 운영을 요구합니다. 보안 기업은 AI의 오용을 방지하고, 투명하고 신뢰할 수 있는 파트너십을 구축해야 합니다. 이를 통해 AI가 발전하는 시대에도 신뢰를 얻고 경쟁력을 유지할 수 있습니다.

Partner Insight

보안 데이터 활용 비즈니스 인텔리전스

영상 감시, 출입 통제, 센서 등 다양한 보안 시스템에서 생성되는 데이터는 단순히 보안을 강화하는 것을 넘어, 비즈니스 성과를 이해하는 데에도 큰 가치를 지닙니다.

소매, 외식, 숙박업 등에서는 사기(fraud)와 손실(shrinkage)이 오랫동안 문제로 이어져 왔습니다.

편의점이나 식당의 경우 직원 부정행위가 전체 손실의 25~45%를 차지합니다.

그렇다면 이러한 손실의 구체적인 원인은 무엇이며, 기업은 이를 줄이기 위해 어떤 구체적인 조치를 취할 수 있을까요?

최근에는 보안 데이터를 기반으로 한 차세대 비즈니스 인텔리전스 도구가 등장하여, 트렌드를 정교하게 분석하고 상황 인식 능력을 향상시키고 있습니다.

예를 들어, 3xLOGIC의 VIGIL TRENDS는 규칙 기반 분석과 추론(inference)을 모두 활용해 내부 절도 패턴을 식별하고, 직원 성과를 최적화하며, 전반적인 운영 효율성을 개선합니다.

한 고객사는 직원 1인당 평균 사기 금액이 800달러에서 500달러로 감소한 결과를 얻었습니다.

데이터의 활용은 보안 시스템에만 국한되지 않습니다. 판매 정보, 날씨 데이터 등 다양한 소스를 통합하면 매장 비교, 매출 전환율, 체류 시간, 방문 트래픽 분석 등 더욱 풍부한 인사이트를 얻을 수 있습니다.

이러한 인사이트는 직접적인 재무적 이익으로 이어질 수 있습니다.

한 3xLOGIC 고객사는 3년에 걸쳐 직원 1인당 평균 사기 금액을 800달러에서 500달러로 줄였습니다. 1000개의 지점을 보유한 체인의 경우, 연간 수만 달러의 손실 방지 효과를 기대할 수 있습니다.

궁극적으로, 보안 중심의 비즈니스 인텔리전스는 기업이 위험을 선제적으로 관리하고, 수익을 보호하며, 청렴한 조직 문화를 구축할 수 있도록 돕습니다.

Partner Insight

OpenEye

오픈 비디오 플랫폼을 통한 비즈니스 인사이트 강화

클라우드 비디오용 오픈 플랫폼을 선택하면 운영 전반의 다양한 데이터를 영상과 결합하여 비즈니스를 보다 완전하게 이해할 수 있는 통합된 관점을 확보할 수 있습니다.

이러한 통합 솔루션은 더 나은 의사결정, 운영 효율성 향상, 그리고 수익성 개선을 가능하게 합니다.

오픈 플랫폼은 출입 통제, 환경 센서, POS(판매 시점 정보 관리), 비즈니스 인텔리전스 등 다양한 비즈니스 시스템을 원활하게 통합하여 보안과 운영을 모두 강화합니다.

이러한 통합은 기존 영상의 단순 기록 용도를 넘어, 실행 가능한 인사이트(Actionable Intelligence)를 제공합니다.

예를 들어, 제조 현장에서는 재고 수준과 직원 활동을 실시간으로 모니터링하여 효율성을 높일 수 있습니다.

연결된 보안 시스템은 조직 전체에 가치를 더합니다.

서비스 운영에서는 거래 데이터와 고객 행동 패턴을 분석해 전략적 조정을 통해 성과와 매출을 향상시킬 수 있습니다.

마케팅과 영업 부문에서는 고객의 상호작용과 선호도를 더 깊이 이해하여 맞춤형 전략을 수립할 수 있습니다.

비즈니스에 가장 중요한 시스템 데이터를 연결하고 분석함으로써, 오픈 플랫폼은 보다 완전한 통합 보안 솔루션을 제공합니다.

연결된 보안 시스템은 조직 전반에 가치를 더하며, 중요한 인사이트를 제공해 더 나은 의사결정을 지원합니다.

비즈니스를 보다 깊이 있게 이해함으로써 보안을 강화하고, 수익성을 높이며, 기업 성장을 가속화할 수 있습니다.

지속가능성과 효율적 운영

지속 가능성(Sustainability)은 많은 조직의 핵심 경영 원칙이자 운영 기준이 되었습니다.

기업들은 환경 발자국을 측정하고 줄이기 위한 구체적인 목표를 설정하고 있습니다.

보안 기술 산업 역시 이러한 변화에 발맞춰 효율성, 확장성, 유연성을 중심으로 발전하고 있습니다.

이를 통해 조직은 지속가능성 목표를 달성하는 동시에 실질적인 비즈니스 이익을 얻을 수 있습니다.

원격 서비스의 이점 실현

산업 전반에서 주목받는 주요 트렌드 중 하나는 '원격 중심(Remote-First)' 접근 방식입니다. 강력한 원격 관리 기능을 갖춘 솔루션과 서비스를 우선시함으로써, 기업은 현장 방문이나 시스템 점검의 필요성을 줄여 탄소 배출을 감소시킬 수 있습니다.

클라우드 기반 보안 시스템은 점점 더 많은 기업이 선호하는 선택지로 자리잡고 있으며, 그 주요 장점 중 하나는 향상된 원격 관리 기능입니다. 특히 여러 지점을 보유한 기업의 경우, 단일 디지털 인터페이스를 통해 전체 보안 활동을 통합 관리할 수 있습니다. 이를 통해 운영의 투명성과 제어력을 높이는 동시에, 현장 인력에 따른 비용을 절감할 수 있습니다.

또한, 원격 모니터링 및 유지관리는 더 빠른 대응, 다운타임 감소, 운영 효율성 향상을 실현하며, 지속 가능성 목표 달성에도 기여합니다.

이러한 접근 방식은 고객과 서비스 제공자 모두에게 이로운 결과를 가져오며, 서비스 품질 향상, 효율적인 운영, 그리고 환경 영향 최소화를 실현합니다.

> "많은 기업이 이제 지속가능성을 핵심 경영 목표로 설정하고 있습니다. Securitas테크놀로지는 고객 및 파트너와의 협력을 통해, 보안 기술을 활용하여 이러한 목표를 달성하도록 지원하고 있습니다."
>
> Kristi Keating | Global VP, Sustainability
> Securitas Technology

친환경 솔루션을 적극적으로 모색하기

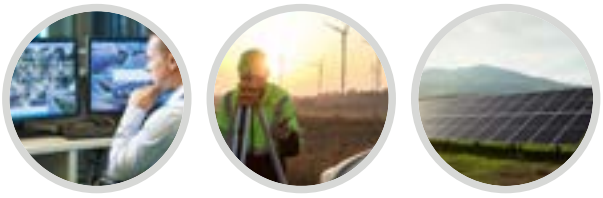
보안 기술의 혁신은 지속가능성 증진에 있어 중요한 역할을 하고 있습니다. 예를 들어, 에너지 효율이 높은 카메라 개발과 LED 장비 사용 확대는 친환경적 해결책을 추구하는 움직임의 일환입니다.

이러한 기술은 에너지 소비를 줄이고 전력 수요를 감소시켜, 기업이 탄소 배출량을 줄이면서 보안 목표와 환경 목표를 동시에 달성할 수 있도록 돕습니다.

지속가능한 데이터의 효율적 관리

SBTi(Science Based Targets initiative)와 같은 국제적 프레임워크에 참여하는 기업들은 환경 영향을 보다 포괄적으로 이해하고 문서화해야 합니다. 여기에는 보안 시스템이 소비하는 에너지 사용량과, 그로 인해 발생하는 간접 배출량(Scope 2)이 포함됩니다.

이러한 배출량을 계산하기 위해서는 장비의 전력 사용량을 파악하고, 그 전력이 어떤 방식으로 생산되는지를 추적해야 합니다.



보안 산업은 이러한 분석을 적극적으로 지원하기 시작했습니다. 북미 지역을 시작으로, 모든 보안 장비의 전력 소비량과 예상 CO2 배출량을 산정하여 고객 견적서에 포함하는 노력을 선도하고 있습니다.

국가별 전력 생산 구조에 기반한 이 데이터는 투명한 지속가능성 관리와 보고 체계 구축에 기여합니다.

또한, 출입 통제 시스템 등 장비의 수명주기(Lifecycle) 전반에 걸친 데이터 관리를 통해, 설치·점검·유지보수 단계별로 발생하는 배출량을 체계적으로 기록할 수 있습니다.

보안산업은 기업들이 지속가능한 목표를 설정하고 달성해 나갈 수 있도록 돕고, 이를 강화하고 지원하는 역할을 수행하고 있습니다.

보안의 우선순위로서의 지속가능성[1]

33%의 보안 전문가들이 지속가능성 관련 활동에 참여하고 있습니다.

48%는 기술 선택 시 지속가능성을 중요하거나 매우 중요하다고 응답했습니다.

지속가능성에 대한 관심은 보안 산업의 패러다임을 바꾸고 있습니다. 운영 효율성과 환경적 이점을 모두 제공하는 혁신이 이루어지고 있으며, 에너지 효율적인 전략과 친환경 기술의 통합을 통해 기업들은 보다 탄력적이고 지속 가능한 미래를 만들어가고 있습니다.

[1]2025년 2월부터 3월까지 호주, 프랑스, 독일, 스웨덴, 영국, 미국의 보안 기술에 대한 의사결정 권한을 가진 보안 전문가 575명을 대상으로 실시된 제3자 블라인드 설문조사.

Partner Insight

간편하고 안전한 시스템 접근을 통한 효율적 워크플로우 지원

빠르게 움직이는 현대의 업무 환경에서는 물리적·디지털 시스템에 신속하고 매끄럽게 접근할 수 있는 환경이 필수적이지만, 보안은 절대 타협할 수 없습니다.

특히 의료 산업과 같은 분야에서는 이러한 요구가 중요합니다. 의료진은 환자 정보와 시스템에 신속하면서도 안전하게 접근해야 하며, 관리자는 자격 증명 관리와 업무 절차 간소화 도구가 필요합니다.

기존의 비밀번호나 PIN 기반 출입 통제 방식은 도난, 분실, 오남용의 위험이 높으며, 실수나 사기가 생명을 위협할 수 있는 의료 환경에서는 충분한 수준의 보안 보장을 제공하지 못합니다.

차세대 출입 통제 기술은 의료 기관을 비롯한 다양한 조직이 접근의 편의성과 보안·통제의 균형을 유지할 수 있도록 지원합니다.

예를 들어, HID OMNIKEY와 같은 통합 신원 인증 플랫폼은 빠르고 안전한 워크스테이션 로그인을 가능하게 하여 시간을 절약하고 데이터 보호를 강화합니다.

이러한 시스템은 다양한 카드 기술을 지원하며 기존 IT 인프라와 원활히 통합되어, 의료 데이터 보호 규정을 준수하면서도 환자 정보에 대한 원활한 접근을 보장합니다.

또 다른 솔루션인 HID DigitalPersona® for Healthcare는 의료 환경의 특수한 접근 문제를 효과적으로 해결합니다.

지문 또는 얼굴 인식과 같은 생체 인증을 통한 싱글 사인온(Single Sign-On) 기능을 제공하여 여러 의료 애플리케이션, 시스템, 물리적 공간에 대한 접근을 간소화합니다.

이를 통해 공유되거나 약한 비밀번호를 제거해 보안을 강화하고, 의료진의 사용자 경험과 업무 효율성을 개선하며, 데이터 보안 및 개인정보 보호 규정 준수를 지원합니다.

또한, 비밀번호 관리에 소요되는 비용을 줄여 상당한 비용 절감 효과를 제공합니다. 워크플로우를 간소화하고 보안을 강화함으로써, 의료 기관은 시스템 로그인에 소비되는 시간을 줄이고 환자 진료와 경험 개선에 더 많은 시간을 투자할 수 있습니다.

Partner Insight

ASSA ABLOY
Opening Solutions

지속가능한 건축물을 위한 보안 기술

엔지니어와 건축가는 건물의 지속가능성 수준(Footprint)을 평가할 때, 건물 전체 구조를 평가하여 에너지 사용 또는 손실이 발생하는 영역을 식별합니다.

기존에는 HVAC(냉난방 공조) 시스템과 단열에 초점이 맞춰졌지만, 최근 새로운 제품이 등장하면서 문이 많은 공간, 잠금장치 및 출입 통제 장비의 에너지 소비 등 다른 고에너지 영역으로 관심이 확대되고 있습니다.

대부분의 건물에는 이미 네트워크 인프라가 구축되어 있습니다.

이러한 기존 IT 네트워크를 출입 통제 등 보안 시스템에 활용함으로써, 에너지 사용을 최적화하고, 배선 및 인건비를 절감하며, 기존 인프라 투자 가치를 극대화할 수 있습니다.

또한 IP 기반 PoE(Power over Ethernet)와 Wi-Fi 잠금 장치는 이러한 과정을 더욱 용이하게 합니다. 기존 IT 인프라를 활용하면 보안 시스템을 쉽게 구현하면서도 비용 효율적으로 확장할 수 있습니다. 보안 기술을 지속가능한 건축 관행에 통합함으로써 효율성과 환경 지속가능성 모두를 향상 시킬 수 있습니다.

건물 소유주들은 탄소 발자국(Carbon Footprint)을 줄이기 위한 지속가능성 목표를 수립하고 있으며, 이러한 목표에 부합하는 제품을 적극적으로 찾고, 유사한 환경 목표를 가진 제조업체와 협력하기를 원합니다.

또한 고객들은 제품의 생산지, 사용된 재료, 제품 수명 주기 전체에서의 에너지 사용량에 대한 투명성을 점점 더 요구하고 있습니다.

당사는 모든 신제품 개발 시 Sustainability Compass(지속가능성 나침반)를 활용하여, 이전 제품보다 더 낮은 환경 영향을 목표로 합니다.

또한 제3자 검증을 받은 지속가능성 인증 문서를 발행하여 고객의 이해를 돕고, 녹색 인증(Green Certification) 취득을 지원합니다.

이러한 투명성과 노력은 고객이 모든 건축 프로젝트에서 지속가능성을 적극적으로 반영할 수 있도록 돕고, 보다 책임 있는 제품을 시장에 공급하도록 이끌고 있습니다.

Partner Insight

보안의 ROI (투자수익률) 탐구

오늘날의 보안 시스템은 기존의 출입 통제와 감시의 영역을 넘어, 비즈니스 운영 효율성을 높이고 투자수익률(ROI)에 긍정적인 영향을 미치는 방향으로 진화하고 있습니다.

이제 보안은 단순한 비용 요소가 아니라, 가치 창출의 전략적 파트너로 자리잡고 있습니다. 사용자와 보안 업체는 이러한 이점을 명확히 측정하고, 이해관계자에게 그 가치를 전달하여 향후 투자에 대한 지지를 확대할 수 있습니다.

영상 감시 및 출입 통제가 ROI를 창출하는 방법

AI와 데이터 분석(Analytics)을 통해 반복적이고 시간이 많이 소요되는 작업을 자동화할 수 있습니다.

이상 행동이 감지되면 자동으로 경보가 생성되어, 운영자는 더 중요한 업무에 집중할 수 있습니다. 이를 통해 운영 효율성과 상황 인식(Situational Awareness)이 향상됩니다.

또한 대응 관리(Response Management) 기능이 강화되어, 차량 색상이나 의류 색상 등 식별 가능한 데이터를 기반으로 현장 인력을 효율적으로 배치할 수 있습니다.

허가되지 않은 인원의 반복적인 접근 시도도 자동으로 감지할 수 있습니다. 카메라는 이동하는 객체를 추적하고, 다른 장치 간 감시 연계를 통해 침입 대응과 경계 통제를 한층 강화합니다.

장기적 가치

출입 통제 시스템을 통해 생성된 시설 사용 데이터 분석은 건물의 효율적 운영에 도움을 줍니다.

예를 들어, 동선 최적화·표지판 배치·청소 및 유지보수 스케줄 개선 등 고객의 이용 패턴에 맞춘 효율적 공간 관리가 가능합니다.

시작하기

타 부서와 협력하면, 보안 리더는 출입 통제와 영상 시스템이 부가 가치를 창출할 수 있는 영역을 식별할 수 있습니다.

이를 통해 보안 팀이 기존에 인지하지 못했던 운영 효율 지표를 발굴할 수도 있습니다.

예: 대기 시간 단축, 일정 최적화, 비용 절감, 안전 개선, 에너지 사용 관리 등. 모든 보안 솔루션을 통합 관리 플랫폼으로 결합하면, 영상·출입 통제·감지·경계 제어 데이터를 한곳에서 관리할 수 있어 효율 개선과 성과 분석이 쉬워집니다.
또한 모든 이해관계자에게 명확하고 일관된 ROI 보고를 제공할 수 있습니다.

Securitas Group Insight

> “직원들이 보호받고 있다고 느낄 때,
> 그들은 직무에 더 오래 머물며 이직률을 낮추고,
> 환자 케어의 질이 향상됩니다.”

Bill McCarthy, President of Securitas Healthcare

Securitas Healthcare

직원 안전 문화를 만드는 일

의료 현장에서 얻은 교훈

의료 현장에서 발생하는 폭력은 세계보건기구(WHO), 유럽연합(EU), 미국 질병통제예방센터(CDC) 등 다양한 기관이 지적한 전 세계적인 문제입니다. 특히 미국에서는 의료 산업이 비치명적 폭력(non-fatal violence)이 가장 많이 발생하는 직종으로, 전체 사례의 무려 73%를[4] 차지합니다.

이러한 이유로, 의료 산업은 직장 내 폭력 위험을 완화하기 위한 체계적이고 강력한 대응 방안을 발전시켜 왔으며, 이는 다른 산업에서도 참고할 수 있는 모델이 되고 있습니다.

“의료 종사자의 안전을 지키기 위해서는 위협의 변화에 맞춰 발전하는 다각적인 접근이 필요합니다. 첨단 보안 기술을 직원 교육 및 훈련과 결합함으로써, 의료진과 환자 모두가 보다 안전한 환경에서 근무하고 치료받을 수 있도록 만들 수 있습니다.”

— Ara Kouchakdjian, VP, Data Intelligence & Healthcare Innovation at Securitas Healthcare.

자세한 내용은 securitashealthcare.com 에서 확인하세요

[1] ‘폭력과 괴롭힘(Violence and Harassment)」, 세계보건기구(World Health Organization),’ 2025. https://www.who.int/tools/occupational-hazards-in-health-sector/violence-harassment
[2] 「직장 내 폭력(Violence in the Workplace)」, 유럽생활근로개선재단(Eurofound), 2023년 2월 27일.https://www.eurofound.europa.eu/en/blog/2023/ violence-workplace-women-and-frontline-workers-face-higher-risks
[3] 「의료 종사자 보호의 우선순위(Prioritising Our Healthcare Workers)」,미국 질병통제예방센터(Centers for Disease Control and Prevention, CDC), 2024년 5월 29일.. https://blogs.cdc.gov/niosh-science-blog/2024/05/29/hcw_violence_mh/
[4] 「의료 분야의 직장 내 폭력(2018년)(Workplace Violence in Healthcare, 2018)」, 미국 노동통계국(Bureau of Labor Statistics), 2020년 4월. https://www.bls.gov/iif/factsheets/workplace-violence-healthcare-2018.htm

다층적 보안 접근 방식

안전한 의료 환경을 유지하기 위해서는 경계 보안, 출입 통제, 실시간 모니터링, 그리고 신속한 대응 체계가 필수적입니다. Securitas Healthcare는 최근 많은 의료 기관들이 법률, 리스크 관리, 보안, 임상 전문가가 함께 참여하는 직장 내 폭력 예방 위원회를 구성하여 종합적이고 다층적인 보안 전략을 수립하는 추세를 확인하고 있습니다.

1

외곽 보안 강화 및 스마트 출입 통제

병원의 보안은 외곽 경계에서부터 시작됩니다. 영상 감시 시스템과 분석 기술을 통해 주차장, 출입구 등 고위험 구역을 실시간으로 모니터링합니다. 움직임 감지 및 얼굴 인식 기술은 실시간으로 위협을 감지해, 사건이 확대되기 전에 보안팀이 즉각 대응할 수 있도록 합니다.

또한, 무기 감지 시스템은 위험 인물이 병원 내부로 진입하기 전에 차단할 수 있으며, 출입 배지 인증 시스템은 인가된 인원만 민감 구역에 접근할 수 있도록 합니다. 방문객 관리 강화를 위해, 병원은 실시간 위치 추적 및 알림 시스템을 도입하여 누가 병원에 출입하고 있는지에 대한 가시성을 확보하고 있습니다.

2

직원 보호: 안전과 유지의 핵심 요소

아무리 강력한 경계 방어가 있더라도, 의료 종사자는 여전히 폭력에 취약합니다. 폭력은 예측할 수 없으며, 보안 요원이 항상 모든 곳에 있을 수는 없습니다. 따라서 병원은 직원 보호 솔루션(Staff Protection Solution)에 적극적으로 투자하고 있습니다.

예를 들어, 긴급 호출 버튼이 내장된 웨어러블 배지(Wearable Badge)는 Securitas Healthcare의 직원 보호 시스템의 대표적인 사례입니다. 이 장치는 직원이 은밀하게 도움을 요청할 수 있도록 하여, 위기 상황 시 즉각적인 지원을 가능하게 합니다.

3

갈등 완화(De-escalation) 교육 및 비상 대응 훈련 강화

기술만으로는 충분하지 않습니다. 직원들은 공격적인 상황을 인식하고, 갈등을 완화하는 기술을 배워야 합니다. 갈등 완화 교육(De-escalation Training)은 직원들이 조기 경고 신호를 인식하고 긴장된 상황을 완화할 수 있도록 돕습니다.

또한, 병원은 정기적으로 비상 대응 훈련(Emergency Preparedness Drills)을 실시합니다. 이는 무장 침입, 대규모 인명 피해, 직장 내 폭력 상황에 대비해 직원들이 위기 상황에서 자신의 역할을 명확히 이해할 수 있도록 합니다.

"직원들이 보호받는다고 느낄 때, 그들은 업무에 더 오래 머물며 이직률이 감소하고 환자 케어의 질이 향상됩니다."
— Bill McCarthy, Securitas Healthcare 대표

"적극적인 보안 조치와 종합적 보안 전략에 투자함으로써, 병원은 직원들이 존중받고, 보호받으며, 최고의 케어를 제공할 수 있는 환경을 조성할 수 있습니다."

보안 전문가를 위한 실행 계획

"보안 기술은 이제 사람과 자산을 보호하는 본래의 사명에 더해, 비즈니스 가치를 창출하는 핵심 요소로 자리 잡고 있습니다.

AI 기반 솔루션과 분석 기술, 원격 서비스, 그리고 지속 가능한 기술에 대한 전략적 투자를 통해 조직은 운영 효율성을 높이고, 보안·비즈니스·환경 목표를 동시에 달성할 수 있습니다."

Doug Walsh | Global VP, Technology Strategy
Securitas Technology

1 보안 데이터의 ROI 중심 활용 사례 개발

운영, 재무, 그리고 기타 부서와 협력하여 보안 시스템 데이터가 조직의 구체적인 목표를 어떻게 지원할 수 있는지 검토합니다.

예를 들어, 손실 감소, 대기 시간 단축, 안전 리스크 식별 등이 있습니다. 이러한 활용 사례를 정의하고, AI 기반의 데이터 분석 인프라를 구축하여 인사이트를 도출하고, 업무 효율성을 높이며, 보안 투자에 대한 확장된 가치를 입증합니다.

2 클라우드를 통한 원격 서비스 활용

보안 시스템을 지원하기 위한 다양한 원격 서비스(Remote Services)에 대해 알아보고 원격 관리(Remote Management) 또는 예방적 유지보수(Preventive Maintenance) 등을 클라우드 전환 로드맵에 반영하여, 원격 중심(Remote-first) 접근 방식이 운영 효율성 및 지속 가능성 향상에 어떻게 기여할 수 있는지 고려합니다.

3 보안이 지속 가능성 목표를 지원하는 방법 이해

조직 내 지속 가능성(Sustainability) 담당자와 협력하여, 보안 기능에서 필요한 데이터가 무엇인지 정의합니다. 이 과정에는 보안 장비의 전력 사용량을 문서화하는 작업이 포함될 수 있습니다.

이는 보안 기술의 환경적 영향(Environmental Footprint) 중 큰 부분을 차지합니다. 또한, 보안 기술 통합업체 및 공급업체와 협력하여 이 데이터를 효율적으로 보고할 수 있는 절차를 구축함으로써, 보안 운영이 지속 가능성 목표와 일치하도록 유지할 수 있습니다.

시큐리타스 테크놀로지 소개

Securitas Technology는
Securitas Group의 한 사업 부문으로,
모든 규모와 유형의 기업을 보호 · 연결 ·
최적화하는 통합 보안 솔루션의
세계적 선도 업체입니다.

40개국에서 13,000명 이상의 전문가와 함께,
우리는 최첨단 보안 기술과
고객 성공에 대한 확고한 헌신을 통해
세상을 더 안전한 곳으로 만드는 것을
사명으로 삼고 있습니다.

Securitas Technology

See a different world

서울특별시 강남구 영동대로 422,
ILWON빌딩 4층 & 6층 (06174)

securitas.kr