

백서

# 레거시 출입통제 시스템의 사이버 보안 위험





# 목차

개요	5
서론	6
레거시 출입통제 시스템의 사이버 보안 취약점	8
크리덴셜 수준의 취약점	10
컨트롤러 수준의 취약점	12
서비스 또는 워크스테이션 수준의 취약점	13
출입통제 시스템의 사이버 보안 모범 사례	14
사이버 보안 이상의 기능을 제공하는 최신 출입통제 시스템	16
도어를 잠그고 여는 것 이상의 이점을 제공하는 최신 출입통제 시스템	20
결론	22



# 개요

대부분의 조직에서 사용하는 출입통제 시스템은 15년 이상 된 것들입니다. 사용 중인 출입통제 시스템으로도 직원들이 문제없이 출입할 수 있는 것처럼 보이지만, 기존 유형의 레거시 기술은 사이버 위협에 취약할 수 있습니다.

사이버 보안이 강화된 최신 출입통제 솔루션은 종단간 암호화와 고급 인증 기능이 있으며, 그 외에도 사이버 공격과 맬웨어를 막는 기능이 있습니다. 최신 융합형 출입통제 방식은 사이버 위협에 대한 조직의 회복 탄력 수준을 강화하면서 단순히 도어를 잠그고 여는 수준을 넘는 더 큰 가치를 구현할 수 있습니다.

1

# 서론

전 세계의 발빠른 사이버 범죄자들이 시설, 감시 시스템, 민감한 데이터에 접근하여 암시장에서 거래하거나 조직을 갈취하는 데 사용할 목적으로 보안 공백을 노리고 있습니다. 침해를 받은 조직들이 거액을 지불하는 가운데, 데이터 침해에 따른 평균 비용이 2020년 386만 달러에서 2021년 424만 달러로 증가했으며<sup>1</sup>, 일부 기업은 이 비용이 수천만 달러에 달했습니다. 2021년에 한 회사는 7000만 달러를 요구받았는데<sup>2</sup> 이 금액은 사이버 공격 조직에서 요구한 최고 금액입니다.

컴퓨터와 서버만 사이버 공격에 취약한 것이 아닙니다. 사이버 보안에서는 인터넷이나 LAN에 연결되어 있는 모든 기기가 취약점이 될 수 있습니다.

레거시 출입통제 시스템의 취약성으로 인해 사이버 보안까지 취약해질 수 있으며, 결국 조직이 위험에 처할 수 있습니다. 최근의 사이버 위협은 크리덴셜, 컨트롤러, 서버 또는 워크스테이션의 각 수준에서 이러한 취약성을 겨냥할 수 있습니다.

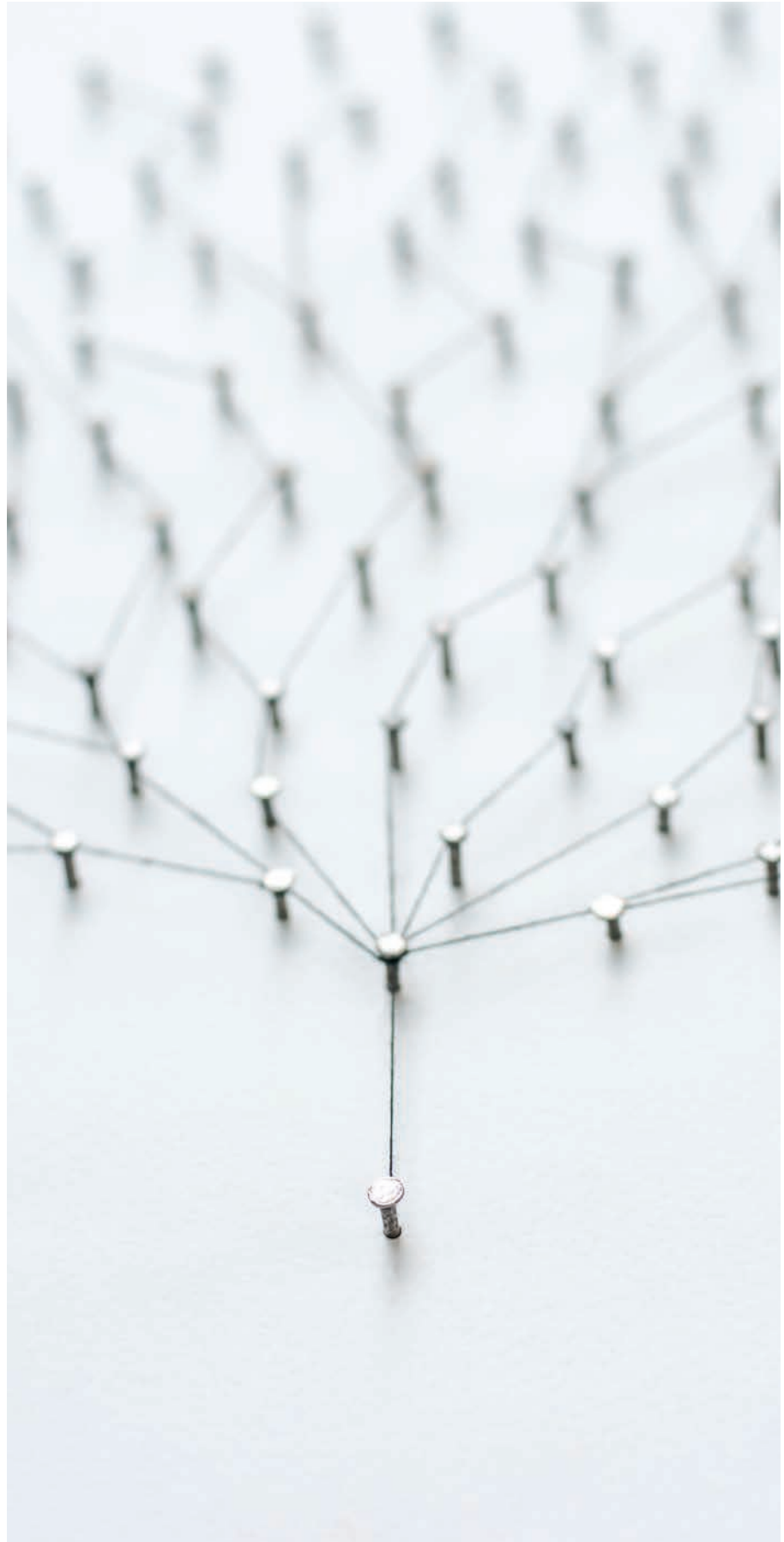
영업 정보나 고객들의 개인정보 같은 민감한 데이터에 접근하기 위해 해커가 네트워크에 침입할 경우 출입통제 시스템의 사이버 보안 침해는 도어의 범위를 한층 초월하는 피해로 이어질 수 있습니다. 이러한 피해로 인해 수익에 영향이 갈 뿐만 아니라 귀사와 직원의 평판, 고객의 프라이버시 등에도 악영향을 줄 수 있습니다.

귀사를 지키기 위해 사이버 보안 솔루션을 강화해야 합니다. 기업, 정부, 학교 및 공공 안전 기관들이 특정 제조사 기반의 독점 솔루션에서 보안 출입통제 솔루션으로 이동하는 이유가 여기에 있습니다. 이들은 사이버 보안을 염두에 두고 구축된 융합형 물리적 보안 플랫폼을 찾고 있습니다.

<sup>1</sup> <https://www.ibm.com/security/data-breach>

<sup>2</sup> <https://www.welivesecurity.com/2021/09/30/eset-threat-report-t22021/>

영업 정보나  
고객들의 개인정보  
같은 민감한  
데이터에 접근하기  
위해 해커가  
네트워크에 침입할  
경우 출입통제  
시스템의 사이버  
보안 침해는  
도어의 범위를  
한층 초월하는  
피해로 이어질 수  
있습니다.



2

## 레거시 출입통제 시스템의 사이버 보안 취약점

현재 대부분의 출입통제 시스템은 인터넷 프로토콜 (IP)에 기반하며, 인터넷을 통해 LAN에 연결됩니다. IP 기반 시스템은 강력하지만 레거시 시스템에는 계속 진화하는 사이버 위협을 막는 데 필요한 사이버 보안 기능이 없습니다.

가장 취약한 링크의 보안 능력이 귀사 출입통제 시스템의 보안 능력이 되는 것입니다. 사이버 범죄자들은 출입통제 시스템에서 네트워크에 연결된 크리덴셜, 컨트롤러, 서버, 워크스테이션의 취약성을 이용할 수 있습니다. 누군가 귀사 네트워크에 침입했다면 이제 침입자는 다른 건물의 시스템을 제어할 수 있습니다. 또한 내부 기록에 있는 민감한 정보를 보거나 훔치는 것은 물론 주요 시스템을 오프라인으로 전환하는 공격을 시작할 수 있습니다.

출입통제 시스템과 관련된 일반적인 사이버 보안 위협은 다음과 같습니다.

- **중간자 공격** — 사이버 범죄자가 네트워크에 접근하여 도어 개방 코드나 기기 로그인 및 비밀번호 같이 기기 사이에서 교환되는 정보를 수집하는 경우입니다.
- **스키밍 및 재전송 공격** — 범죄자가 자신의 리더기를 사용해 무단으로 피해자의 카드에 접속해 정보를 복제하는 경우입니다.
- **컨트롤러 공격** — 범죄자가 컨트롤러 펌웨어를 덮어써서 기기를 사용할 수 없게 만드는 경우입니다.

누군가 귀사  
네트워크에  
침입했다면  
이제 침입자는  
다른 건물의  
시스템을 제어할  
수 있습니다. 또한  
내부 기록에 있는  
민감한 정보를  
보거나 훔치는 것은  
물론 주요 시스템을  
오프라인으로  
전환하는 공격을  
시작할 수  
있습니다.



3

## 크리덴셜 수준의 취약점

출입통제 시스템은 사용자 크리덴셜로 특정 구역에 출입할 수 있는 사람인지 여부를 판단합니다. PIN 코드, 스마트폰 앱, 지문, 스마트 키, 카드를 포함해 출입통제 시스템에서 사용되는 크리덴셜 종류는 다양합니다.

사이버 범죄자는 스키밍 공격으로 사용자 크리덴셜을 훔칠 수 있습니다. 이렇게 이들은 권한이 없는 자신의 리더기를 사용해 사용자 몰래 정보에 접근하는 것입니다. 또는 이들이 귀사 네트워크에 접근할 수 있는 경우에는 네트워크에서 전송된 크리덴셜 데이터를 가로챈 다음 보관했다가 나중에 사용할 수도 있습니다. 사이버 범죄자는 이 데이터를 사용해 아직 사용 중인 오래된 종류의 키 카드나 스마트 키를 '스푸핑(spoofing)'하거나 복제할 수 있습니다. 근접식 카드 같이 오래된 방식의 크리덴셜은 대부분 온라인에서 구입할 수 있는 저렴한 장치를 사용해 아주 쉽게 복사할 수 있습니다.

125kHz 근접식 카드와 마그네틱 스트라이프가 있는 레거시 출입통제 시스템에 흔히 사용되는 일부 크리덴셜에도 취약점이 있습니다. 대부분 Weigand 프로토콜을 통해 통신하는데, 이 프로토콜은 1974년에 고안된 이후 산업 표준이 되었습니다. 안타깝게도 해커들은 이 유형의 시스템에 사용되는 카드 리더기를 조작하여 민감한 정보를 검색하는 방법을 알아냈습니다.

Wiegand 통신은 일방향이기 때문에 리더기가 조작된 경우 탬퍼 스위치에 유선으로 연결된 경우가 아니라면 컨트롤러가 이를 감지하지 못합니다. Wiegand 유형의 시스템을 통해 전송된 데이터는 암호화도 안 되기 때문에 보안 크리덴셜을 사용해도 민감한 정보가 검색될 수 있습니다.

중간자 공격 위험을 낮추기 위해서는 리더기와 OSDP2 같은 컨트롤러 사이에 양방향 보안 프로토콜이 있는 시스템을 사용해야 합니다. 그래야만 누군가 리더기를 조작하거나 가짜 리더기로 바꾸어 크리덴셜을 훔치려고 할 때 민감한 정보를 검색하지 못합니다. 또한 양방향 프로토콜은 시스템 조작

크리덴셜 수준에서  
일반적인 취약점은  
인적 오류입니다.  
PIN 코드나 스마트  
키를 공유하거나  
키 카드 분실 또는  
도어를 받침대로  
고여 열어두는 것이  
이에 해당합니다.

시도가 있었다는 사실을 운영자에게 통지하기 때문에 보안 팀에서 신속하게 대응하여 위협을 무력화할 수 있습니다.

그러나 크리덴셜 수준에서 일반적인 취약점은 인적 오류입니다. PIN 코드나 스마트 키를 공유하거나, 키 카드 분실 또는 도어를 받침대로 고여 열어두는 경우처럼 흔히 저지르는 사소한 잘못이 건물의 보안을 크게 해칠 수 있습니다.

고급 보안 크리덴셜이나 생체인식 장치를 선택하는 것이 크리덴셜 수준의 취약성을 낮추는 가장 좋은 방법입니다. 사이버 보안의 환경을 개선하는 것도 인적 오류와 관련된 위험을 줄이는 데 도움이 될 수 있습니다. 모든 직원에게 교육, 팝업 메시지, 알림 메시지를 제공하여 사이버 보안을 장려하고 강화하는 문화를 조성해야 합니다. 이것은 협력업체에도 적용되어야 합니다. 협력업체 측에서 일어난 침해가 귀사 보안에도 영향을 줄 수 있기 때문입니다. 모든 소프트웨어 파트너사에게 직원들이 사이버 보안 모범 사례를 따를 수 있도록 해당 조치를 명시하도록 요청하고, 새로운 소프트웨어 파트너사나 네트워크 연결식 하드웨어 공급업체와 협의할 때 제안요청서의 요구 사항 중 하나로 사이버 보안을 포함할 것을 요구해야 합니다.

정보를 수작업으로 관리하고 추적할 때 실수하기 쉬운 프로세스 중 하나가 출입권한 관리입니다. 개인이 아닌 역할과 사용자 지위에 따라 출입권한을 관리하는 융합형 솔루션도 제공할 수 있는 보안 파트너를 선택해야 합니다. 그래야만 변경이 필요할 때 자동으로 출입자의 접근권한을 높이거나 낮출 수 있으며 추가 또는 취소할 수 있습니다. 예를 들어, 직원이 출산 휴가를 내거나 역할이 달라지는 사례가 있을 수 있으며 퇴직하는 경우도 있습니다. 이처럼 직원의 지위가 연계된 데이터베이스에서 달라지면 접근권한도 달라져야 하고, 이를 통해 누군가 기존 키 카드를 사용해 본인이 소속되어 있지 않는 구역으로 출입할 위험을 없앨 수 있습니다. 또한 융합형 시스템을 사용하면 키 카드나 크리덴셜 분실 또는 도난이 발생했을 때 신속하게 접근권한을 취소할 수 있습니다.

4

## 컨트롤러 수준의 취약점

컨트롤러는 리더기의 크리덴셜을 판독하고 이것을 출입통제 서버와 동기화된 화이트리스트와 비교합니다. 크리덴셜이 일치하면 도어 잠금장치로 신호를 보내 도어를 열거나 출입을 거부합니다.

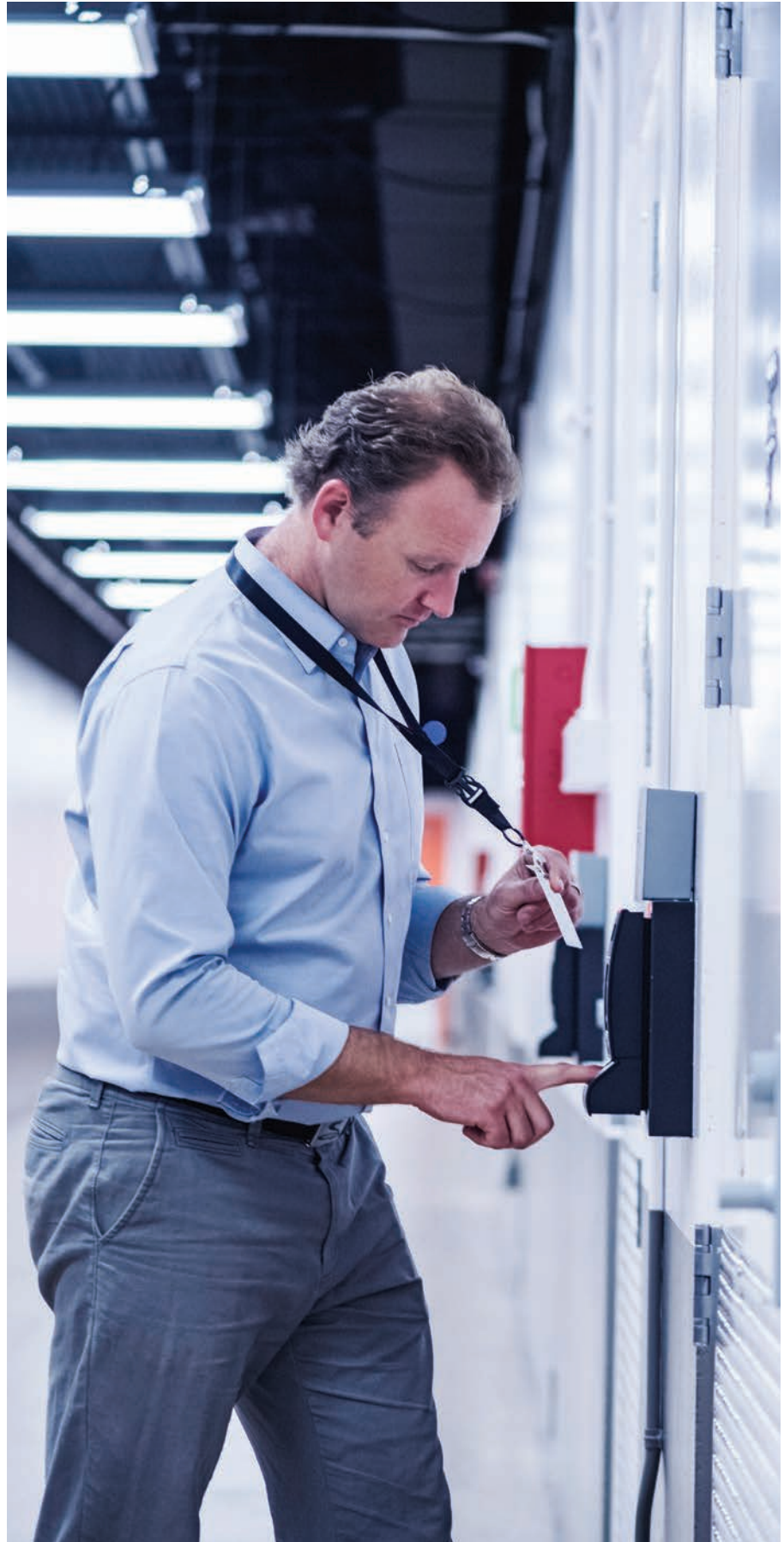
암호화와 비밀번호가 취약하면 사이버 범죄자가 컨트롤러에 대한 접근권한을 획득하여 시설로 들어가는 키를 갖게 될 수 있습니다.

최신 출입통제 시스템은 지능형 인증서 관리 도구를 사용해 컨트롤러를 인증하고 출입통제 서버와 컨트롤러 사이의 보안 통신을 보장합니다. 이 인증을 통해 컨트롤러가 적절한 서버에 연결되고 이 서버로부터 명령을 수신하는지 확인하게 됩니다. 이 두 구성요소 사이의 보안 통신이 보장되도록, 전송 계층 보안(TLS) 프로토콜 버전 1.2 이상을 사용해 통신을 암호화하는 것이 좋습니다.

컨트롤러는 정기적으로 펌웨어를 업데이트하여 보안 상태를 최신으로 유지해야 합니다. 보안 팀에서 업데이트가 정기적으로 이루어지는지 확인하거나, 이 작업을 명망 있는 써드파티나 공급업체에 맡겨 업데이트가 신속하게 설치되도록 해야 합니다.

마지막으로 컨트롤러 보안을 위해 취해야 하는 간단하면서도 중요한 조치는 기본 비밀번호가 쉽게 추측할 수 없는 고유한 것으로 변경되었는지 확인하는 것입니다. 장치 사이에서 사용되는 비밀번호를 정기적으로 자동 변경하는 비밀번호 관리 시스템을 갖추는 것도 모범 관행 중 하나입니다.

컨트롤러는 정기적으로 펌웨어를 업데이트하여 보안 상태를 최신으로 유지해야 합니다. 보안 팀에서 업데이트가 정기적으로 이루어지는지 확인하여 신속히 설치되도록 해야 합니다.



5

## 서비스 또는 워크스테이션 수준의 취약점

서버는 승인 후 개인들에게 부여된 크리덴셜 목록을 저장하고 관리하며, 컨트롤러와 통신하여 크리덴셜 데이터를 인증합니다. 이 정보는 네트워크를 통해 전송되어야 합니다. 데이터가 암호화되지 않으면 네트워크에 접근할 수 있는 사이버 범죄자들이 크리덴셜 정보와 기타 민감한 데이터를 가로챌 수 있습니다.

리더기에서 수집되어 서버에 저장되는 크리덴셜 데이터는 강력한 암호, 인증 및 승인 방법으로 보호해야 합니다. 서버 수준의 취약점 대부분은 다음에 관한 것입니다.

- 허가받지 않은 사용자가 취약한 인증 방법을 사용하는 경우
- 사용 권한이 너무 관대해서 제한해야 하는 데이터에 접근하거나 시스템을 무단으로 변경할 수 있는 경우
- 승인된 사람만 민감한 정보를 볼 수 있도록 서버가 사용자 인증을 관리하는 능력

리더기에서  
수집되어 서버에  
저장되는 크리덴셜  
데이터는 강력한  
암호, 인증 및 승인  
방법으로 보호해야  
합니다.



6

## 출입통제 시스템의 사이버 보안 모범 사례

최근 몇 년에 걸쳐 출입통제 기술에 엄청난 변화가 있었습니다. 그동안 독점이었던 이 시장이 보다 개방적인 시장으로 변했습니다. 이제는 고객들이 하나의 공급업체에 종속되지 않아 기업들이 더 혁신적인 제품과 서비스를 개발하고 있습니다. 이렇게 사이버 보안이 강화된 최신 솔루션은 종단간 암호화와 고급 인증 기능이 있으며, 그 외에도 사이버 공격과 맬웨어를 막는 기능이 있습니다.

### 귀사 네트워크의 사이버 보안을 개선하려면

- 시스템을 업그레이드해야 합니다. 오래된 시스템으로는 현재의 위협에 대응하지 못합니다.
- 안전한 스마트 및 모바일 크리덴셜과 최신 통신 프로토콜을 사용해 인터넷을 통해 전송되는 데이터를 보호해야 합니다.
- 직원 교육을 통해 사이버 보안 모범 사례를 알리고 비밀번호를 업데이트하라는 메시지를 자주 전달해야 합니다.
- 신원 관리 시스템을 사용해 직원의 역할과 현재 지위와 관련된 구역 및 데이터에만 접근할 수 있게 해야 합니다.
- 고도로 민감한 정보를 저장하거나 공유하는 기기의 전용 로컬 네트워크를 구축해 일반 네트워크에서 접근하지 못하게 해야 합니다.
- 정립된 보안 관리 체계를 준수한다는 것을 입증할 수 있는 보안업체를 선택해야 합니다.

대부분의 조직은 하이브리드 방식을 선호하기 때문에 클라우드 소프트웨어 및 데이터 스토리지 옵션의 유연성과 확장성을 이용하면서 로컬에서 관리하는 서버도 관리할 수 있습니다.

- 출입통제 시스템에서 검증된 데이터 암호화 방법과 다중 인증을 사용해야 합니다.
- 사이버 위협을 모니터링하고 소프트웨어를 빈번히 업데이트할 수 있으며 필요 시 패치 적용이 가능한 전담 팀을 갖춘 파트너사와 협업해야 합니다.

클라우드 기반 또는 온프레미스 솔루션 중에서 하나를 선택할 필요가 없습니다. 대부분의 조직은 하이브리드 방식을 선호하기 때문에 클라우드 소프트웨어 및 데이터 스토리지 옵션의 유연성과 확장성을 이용하면서 로컬에서 관리하는 서버도 관리할 수 있습니다.

7

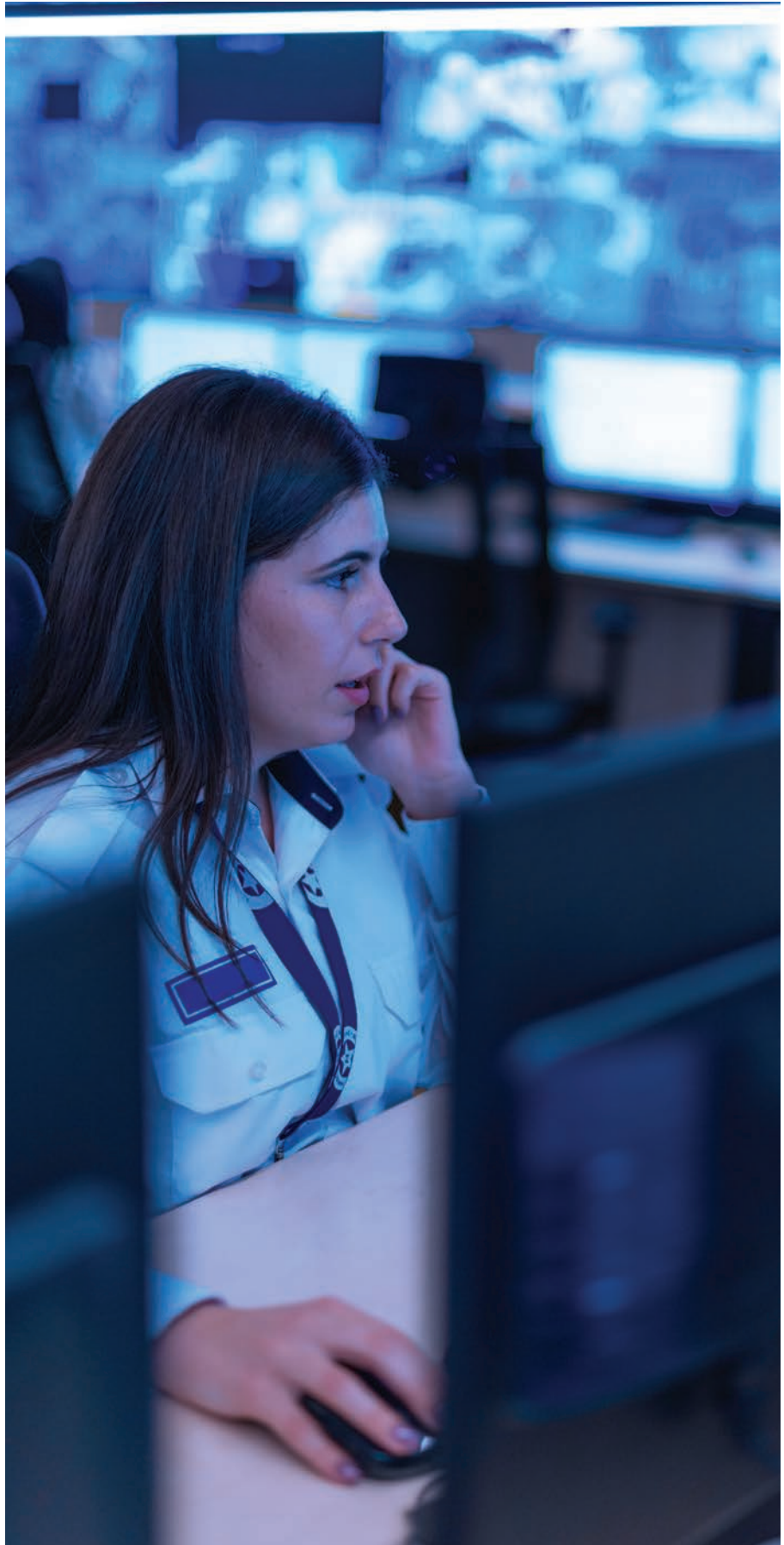
## 사이버 보안 이상의 기능을 제공하는 최신 출입통제 시스템

Genetec Security Center Synergis 같이 통신, 서버 및 데이터를 보호하기 위해 최신 사이버 보안 표준을 사용하는 융합형 출입통제 시스템은 조직의 자산과 직원을 더 잘 보호할 수 있을 뿐만 아니라 도어를 잠그고 여는 차원을 넘어 사업 운영과 의사결정까지 개선하는 데 도움을 줄 수 있습니다. 오픈 아키텍처 IP 기반의 출입통제 시스템을 선택한 조직은 언제든지 최신 지원 기술로 업그레이드할 수 있으며, 조직의 상황에 맞는 속도로 개선하고 가용 예산 내에서 작업할 능력을 갖게 됩니다.

[Synergis™ 출입통제](#) 시스템은 최신 사이버 보안 표준을 사용해 아키텍처의 각 수준에서 통신, 서버 및 데이터를 보호합니다. 출입 카드에서 소프트웨어에 이르기까지 고급 보호 기능을 사용하기 때문에 엿보는 사람을 염려할 필요 없이 건물에 확실하게 출입할 수 있습니다.

[Genetec™ Security Center](#)는 IP 기반 VMS, 출입통제, 자동 번호판 인식 솔루션(ALPR), 통신 및 영상분석을 융합하는 오픈 아키텍처 플랫폼입니다. 또한 정부, 기업, 교통 및 우리가 살아가는 공동체의 보안을 강화하고 새로운 수준의 운영 인텔리전스를 제공하기 위해 클라우드 기반의 솔루션과 서비스를 개발합니다.

Security Center는  
IP 기반 VMS,  
출입통제, 자동  
번호판 인식  
솔루션(ALPR),  
통신 및  
영상분석을  
융합하는 오픈  
아키텍처  
플랫폼입니다.



8

## 도어를 잠그고 여는 것 이상의 이점을 제공하는 최신 출입통제 시스템

Synergis 같은 최신형 사이버 보안 출입통제 시스템은 특정 일정에 따라 단순히 도어를 잠그고 여는 것 이상의 일을 해낼 수 있습니다. 출입통제 시스템이 수집한 수많은 데이터를 사용하여 이 데이터에 다른 출처의 데이터를 결합하고 효과적인 새로운 통찰 정보를 확보함으로써 보안은 물론 일상의 운영까지 개선하는 데 도움을 줄 수 있습니다. 따라서 최신형 보안 시스템의 투자 수익률은 훨씬 더 높습니다.

Synergis는 도어를 넘어 새로운 통찰을 얻는 문까지 열어주어 의사결정과 일상 운영을 개선하는 데 도움을 줍니다. 또한 진정한 개방형 시스템이기 때문에 널리 사용되고 있는 타사 출입통제 장치와 연결되며, 데이터를 동적 형식으로 집계하고 표시하여 보다 스마트하게 사업을 영위할 수 있도록 지원합니다.

예를 들어, 코로나 팬데믹 기간에 Synergis 고객들은 새로운 생체 인식 리더기를 신속 간편하게 설치하여 물리적 접촉의 필요성을 줄임으로써<sup>3</sup> 바이러스 확산을 제어할 수 있었습니다. 또한 이들은 출입통제 시스템 데이터를 사용해 직원이 양성 확진을 받은 경우 접촉자 추적<sup>4</sup>을 지원했을 뿐만 아니라, 공중보건 당국에서 요구하는 물리적 거리두기<sup>5</sup>와 공간 점유 수준도 관리할 수 있었습니다.

실시간 점유  
관리에서 원격  
인프라 모니터링에  
이르기까지  
Synergis를 통해  
도어뿐만 아니라  
사업 운영까지  
효율적으로 지킬  
수 있습니다.

출입통제 시스템은 데이터를 다량 수집하지만, 오래된 시스템은 데이터를 수집하고 파악하는 것이 어렵습니다. Synergis에는 모든 보안 시스템과 센서 데이터를 통합하여 볼 수 있는 대시보드로 추세를 파악하기 때문에, 운영 결정에 따른 사후 대응이 아닌 사전 대응이 가능합니다.

실시간 점유 관리에서 원격 인프라 모니터링에 이르기까지 Synergis를 통해 도어뿐만 아니라 사업 운영까지 효율적으로 지킬 수 있습니다. 소프트웨어 설정을 조정하거나 하드웨어를 추가하고 업그레이드하기가 쉬워 변화하는 요구에 맞게 처리할 수 있기 때문에, 전체 시스템을 바꿀 필요가 없습니다. 출입통제 데이터를 사용해 건물 자동화를 지원하거나 사람들이 없을 때 전등을 끌 수 있으며 냉난방을 조정할 수 있습니다. 또한 건물에서 가장 많이 사용되는 구역을 명확히 파악할 수 있어, 필요하다고 생각하는 공간의 규모가 적절한지 판단할 수 있습니다.

<sup>3</sup> <https://www.genetec.com/podcasts/engage/episode-10-stepping-up-cybersecurity-biometrics-and-multifactor-authentication>

<sup>4</sup> <https://www.genetec.com/press-center/press-releases/2021/02/genetec-helps-westminster-property-ventures-ensure-safe-return-to-work-for-its-commercial-tenants>

<sup>5</sup> <https://resources.genetec.com/en-industry-focuses/genetec-occupancy-management-package>

9

## 결론

[Security Center Synergis](#) 같이 통신, 서버 및 데이터를 보호하기 위해 최신 사이버 보안 표준을 사용하는 융합형 출입통제 시스템은 조직의 자산과 직원을 더 잘 보호할 수 있을 뿐만 아니라 도어를 잠그고 여는 차원을 넘어 사업 운영과 의사결정까지 개선하는 데 도움을 줄 수 있습니다. [오픈 아키텍처 IP 기반의 출입통제 시스템을 선택한](#) 조직은 언제든지 최신 지원 기술로 업그레이드할 수 있으며, 조직의 상황에 맞는 속도로 개선하고 가용 예산 내에서 작업할 능력을 갖게 됩니다.

### 자세한 내용을 보시려면

IP 기반 출입통제 시스템으로 이동할 때 고려해야 하는 상위 7개 사항에 관한 체크리스트를 다운로드하세요.

체크리스트 받기

Genetec은 보안, 운영 및 인텔리전스 부문을 아우르며, 광범위한 솔루션 포트폴리오를 보유한 혁신적인 테크놀로지 기업입니다. Genetec의 주력 제품인 Genetec™ Security Center는 IP 기반의 VMS, 출입 통제, 자동 번호판 인식 솔루션(ALPR), 통신 및 분석을 융합하는 물리적 보안 플랫폼입니다. 또한 정부, 기업, 교통 및 우리가 살아가는 공동체의 보안을 강화하고 새로운 수준의 운영 인텔리전스를 제공하기 위해 클라우드 기반의 솔루션과 서비스를 개발합니다. Genetec은 1997년에 설립되어 캐나다 몬트리올에 본사를 두고 있으며, 159여 개 국가의 재판매업자, 연동업체, 공인 채널 파트너 및 컨설턴트로 구성된 방대한 네트워크를 통해 전 세계의 고객에게 서비스를 제공하고 있습니다.

**VMS:** 기관과 조직 간에 카메라를 공유할 수 있으며, 공통 운영 상황을 제공하여 사고 대응 시간을 단축함으로써 상황 인식을 개선하고 도시 내 보안을 강화할 수 있습니다.

**출입통제:** 새로운 출입통제 시스템을 설치하든 기존에 설치된 소프트웨어를 업데이트하든 관계없이, IP 기반의 융합형 플랫폼으로 조직의 보안을 강화하고 위협에 효과적으로 대응하며 더 명확하고 시기 적절한 결정을 내릴 수 있습니다.

**자동 번호판 인식 솔루션:** 소유권과 개인정보를 침해하지 않을 뿐 아니라, 선택된 기관 및 파트너 조직과 번호판 데이터를 공유하는 기능을 통해 관심 차량의 감지를 자동화하고 불법 주정차 단속의 효율을 높이며 공공 안전 조사를 강화할 수 있습니다.

#### **운영 의사결정 지원:**

상황 경고는 물론 정책 기반 절차를 통해 상세 사례를 출력하는 기능에 이르기까지 운영자를 지원하는 고급 워크플로를 통해 사건 처리와 의사 결정에 효율성을 더합니다.

**조사 사례 관리 솔루션:** 디지털 증거를 중앙 집중화하고 조사관, 외부 기관 및 대중과 안전하게 협업할 수 있도록 지원하는 플랫폼 덕분에 사건조사 관리를 간소화하고 조사 시간을 단축합니다.

**클라우드 서비스:** 빠른 속도로 변화하는 보안 요건에 쉽게 대응하고 더 높은 운영 효율성을 제공하는 확장성이 뛰어난 주문형 클라우드 서비스를 통해 온프레미스 보안 시스템의 기능을 확장하고 IT 비용을 절감합니다.

**Genetec Inc.**  
[genetec.com/locations](https://www.genetec.com/locations)  
[info@genetec.com](mailto:info@genetec.com)  
[@genetec](https://www.genetec.com)

© Genetec Inc., 2022. Genetec과 그 로고는 Genetec Inc.의 상표이며 여러 관할 구역에서 이미 등록되었거나 등록 대기 중일 수 있습니다. 이 문서에 사용된 기타 상표는 해당 제품의 제조업체 또는 공급업체의 상표일 수 있습니다.