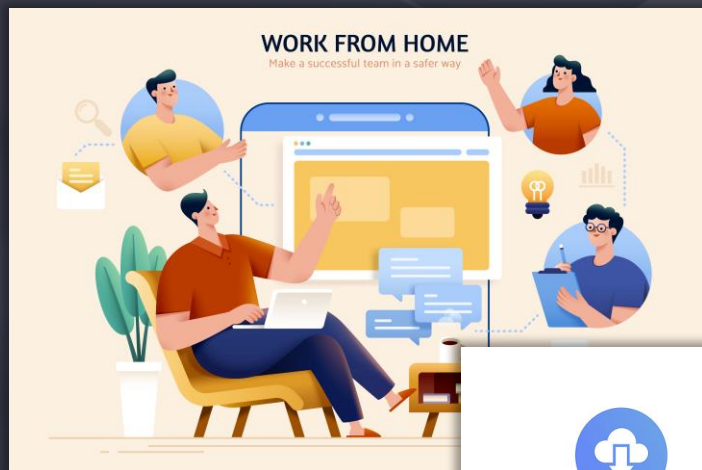


단일 에이전트로 구현한 엔드포인트 보안 통합 사례



투씨에스지 사업전략팀
윤주영 팀장

다양한 형태의 업무 환경



보안 관제 포인트 증가



공격 표면 증가

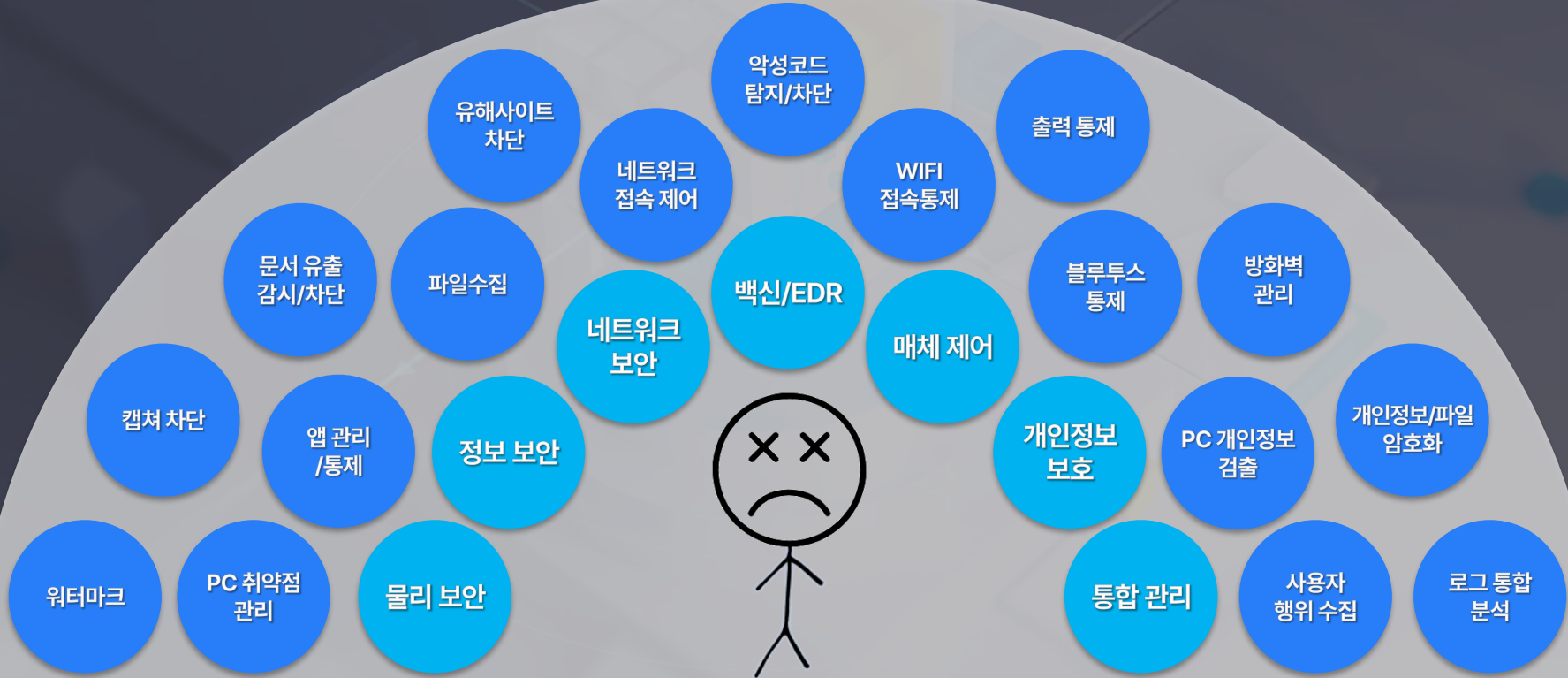


관제 포인트 증가



다양한 보안 이벤트
분석 필요

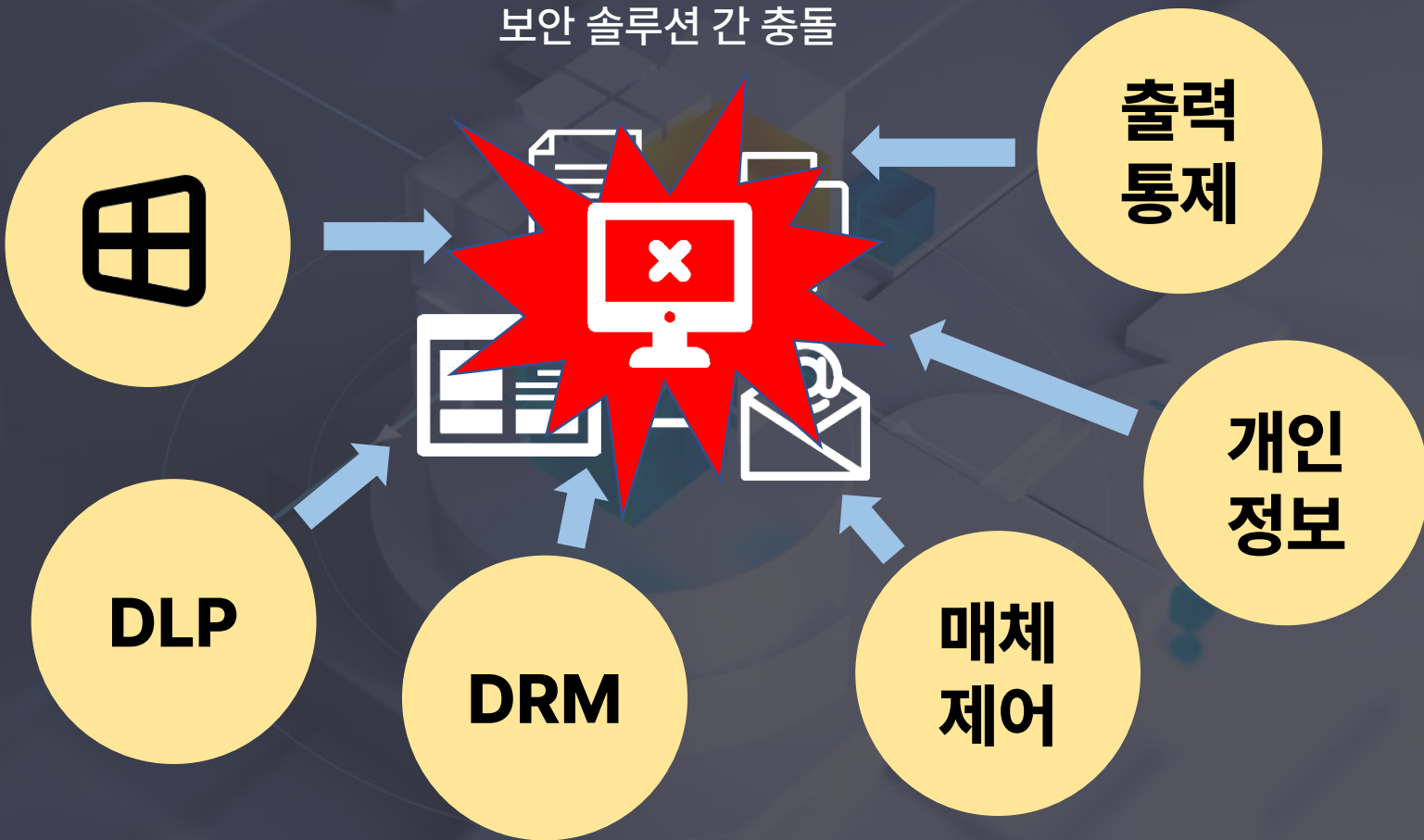
現 엔드포인트 보안 솔루션 현황



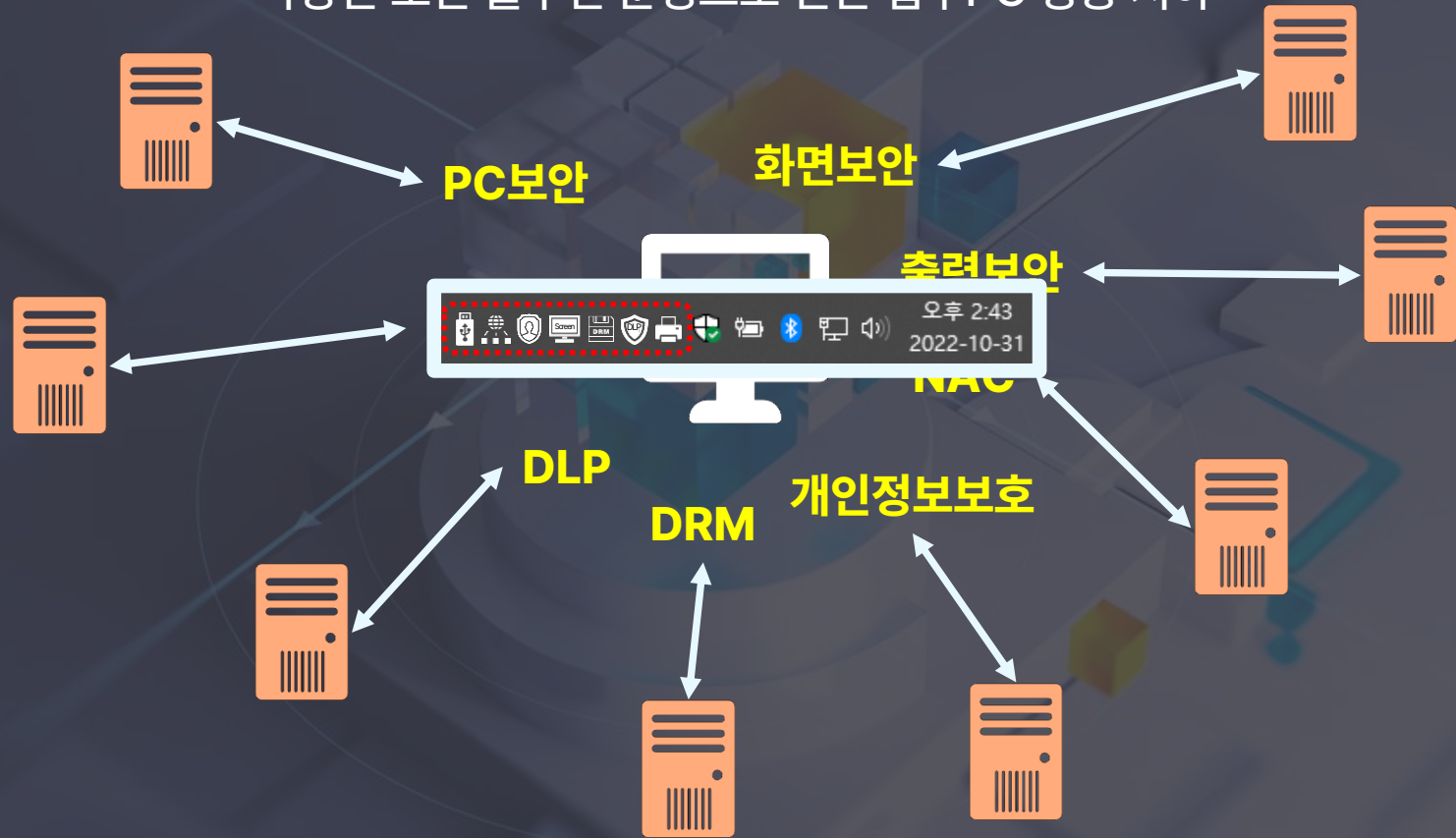
The background is a dark, muted blue-grey color. It features a complex, abstract 3D geometric design. In the center, there's a cluster of light grey and yellow cubes. To the right, a blue cube is visible. Below the central cluster, there's a blue cube with three small blue spheres above it. A yellow cube is positioned at the bottom right. A light blue line with arrows at both ends runs diagonally from the bottom left towards the center. Another light blue line runs horizontally across the middle. A circular light blue line is centered around the main cube cluster. The overall aesthetic is modern and technological.

現 엔드포인트 보안 솔루션 현황 이슈

보안 솔루션 간 충돌



다양한 보안 솔루션 운영으로 인한 업무PC 성능 저하



업무PC 성능 저하로 인한 임직원의 불만



tistory.com

<https://seijitsu.tistory.com> > ...

보안 프로그램 충돌 반복 설치 오류 지긋지긋 하시죠?

2021. 7. 20. — 보안 프로그램 설치 페이지로 들어가면 4~5가지 정도의 보안 프로그램이 있는데
요. 다른 사이트로 들어갔다가 더 낮은 버전으로 다시 깔아버려서 높은 ...

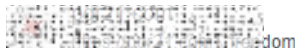


hungryboarder.com

<http://www.hungryboarder.com> > ...

기타물고답하기 - 사내 보안프로그램 아시는 분.

... 보안 프로그램인데, 하도 어이 없어 IT업에 계시는 전문가 ... 귀
... 전이 틀려 두 DRM이 충돌 하는 것이다.



[일반] 보안프로그램 대공해 시대 -

2016. 7. 4. — 쓰는 입장에서 짜증나고, 적응하고 관리하는 입장에서 매우 짜증납니다. ... 심
지어 키보드 보안 프로그램끼리 충돌이 나서 보안프로그램 실행되면 ...

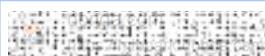


naver.com

<http://m.blog.naver.com/piastarest> > ...

보안 프로그램 설치 후 노트북 Synaptics 터치패드 재부팅 현상

2018. 3. 19. — 그러나 보안 프로그램과 충돌이 있다는 가정하에 프로그램을 하나씩 지워보았다.
... 치 패드를 건드리니 ...

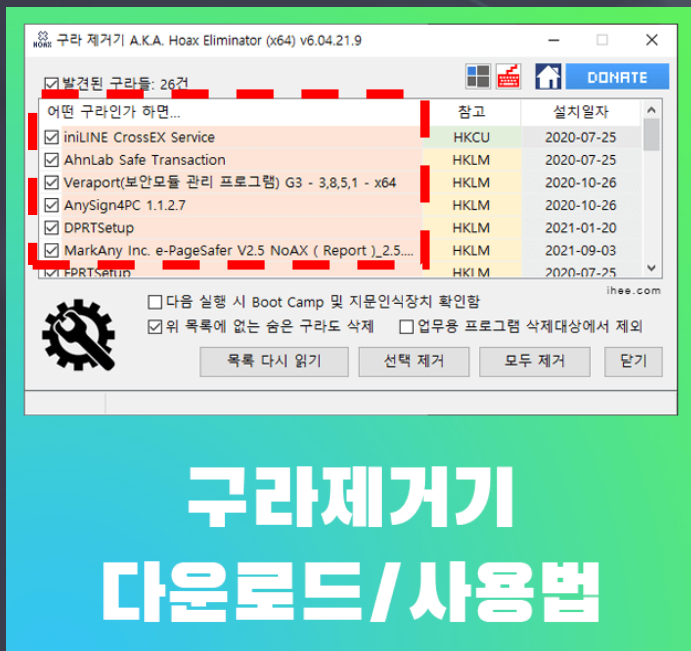


[b.php](#)

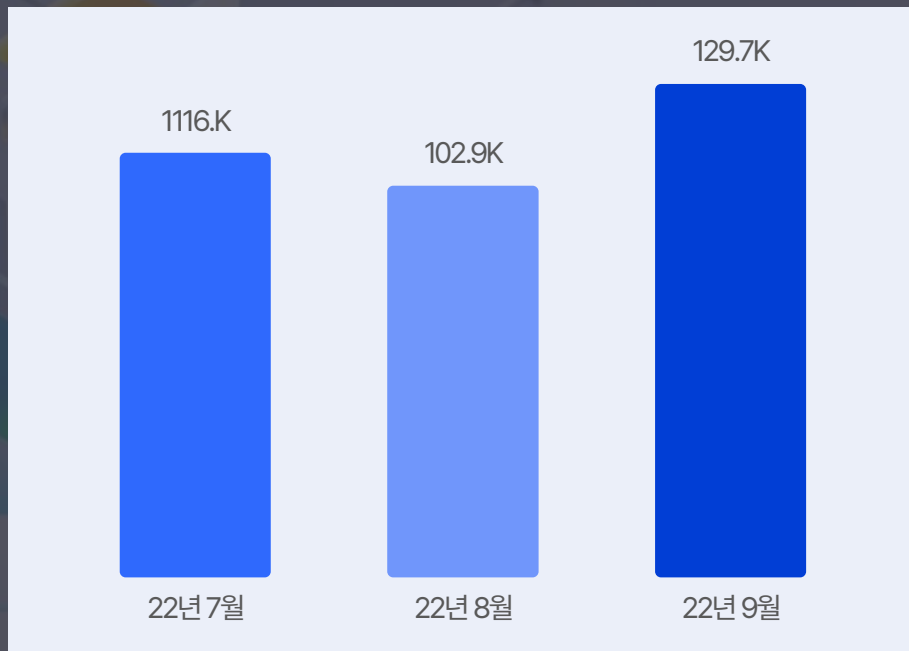
PC 느려짐 주원인이 보안프로그램이었네요. :

별글PC 느려짐 주원인이 보안프로그램이었네요. 2021-02-21 08:03. 경언甲. 추천 0 조회 1,333
리플 4. 가. 가. 특히 금융기관 이용시 자동으로 깔리는 보안 ...

업무PC의 성능 저하를 해결하고자 하는 사용자들의 적극적인 노력



[각종 보안 프로그램 제거 전용 솔루션]



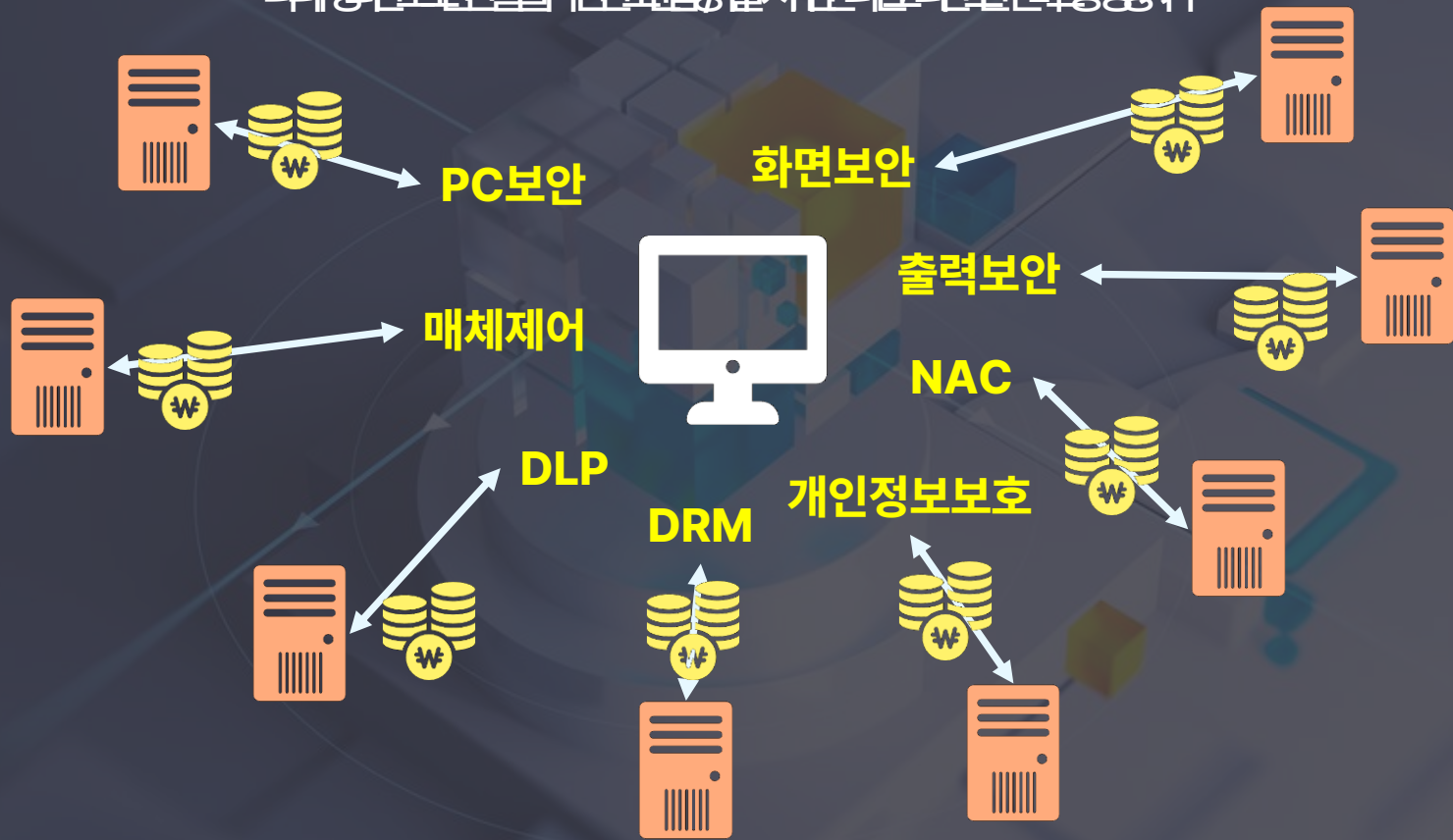
[제거 솔루션 사이트 22년 3/4분기 일평균 방문자 수 약 3,800명]

11/11/2019 11:11:11 AM

100

100

다양한 보안 솔루션 도입 필요성 증가
자율 관리로 인한 비용 증가



경제 상황 악화 등을 비롯한 내외부 여건에 따른 비용 절감 필요성

비즈니스 성공을 저해하는 가장 큰 요인

67%

“보안 침해 및 데이터 유출”

비즈니스 성공을 위한 우선 과제

73%

“비용절감”

The background is a dark, muted blue-grey color. It features an abstract 3D geometric design. In the center, there is a cluster of light grey cubes, some of which are stacked. A prominent yellow cube is visible within this cluster. To the right, there are more cubes, including a blue one. A large, faint, light blue circular arrow or path is visible, curving around the central cube structure. The overall aesthetic is modern and architectural.

“많아서 생기는 문제라면 줄이면 될까?”

문제 해결을 위해 특정 보안 프로그램을 뺀다?



보안이 부족한 상황에서 발생한 보안 사고와는 다른, 보안 담당자의 책임 발생

An abstract 3D geometric composition featuring various cubes and spheres in muted colors like teal, yellow, and grey, arranged in a complex, layered structure. The background is a dark, textured grey with faint, glowing lines and circles, suggesting a technical or architectural theme. The overall aesthetic is modern and minimalist.

“효과적인 이슈 해결 방안은?”

보안 솔루션 통합

PC보안

화면보안

출력보안

매체제어

AC

DLI

인정보보호



보안 솔루션 통합의 조건 #1



One Agent



이름	상태	CPU	메모리
> DLP Agent Process.exe		10%	150MB
> DRM Agent Process.exe		15%	120MB
> Privacy Security Agent Process.exe		12%	80MB
> NAC Agent Process.exe		8%	55MB
> Printer Monitoring.exe		9%	76MB



이름	상태	CPU	메모리
> In-house & Remote work secur...		0.1%	19.3MB

보안 솔루션 통합의 조건 #2



One Console



DLP
DRM
NAC
매체제어
PC보안
화면보안
출력보안
개인정보보호
⋮



보안 솔루션 통합의 조건 #3



Seamless log



솔루션이 아닌 사용자를 기준으로 가시성 높은 보안 이벤트 수집/제공할 수 있어야 함

보안 솔루션 통합의 조건 #3

사내망 접속

접속 로그

시스템 로그

사용자 행위 로그

사용자 기준의
접속로그/시스템로그/행위로그

로그아웃

VPN

A

B

C

VDI(OS)

DLP/DRM/매체제어/...

사내망 접속

시스템/행위
로그

로그아웃

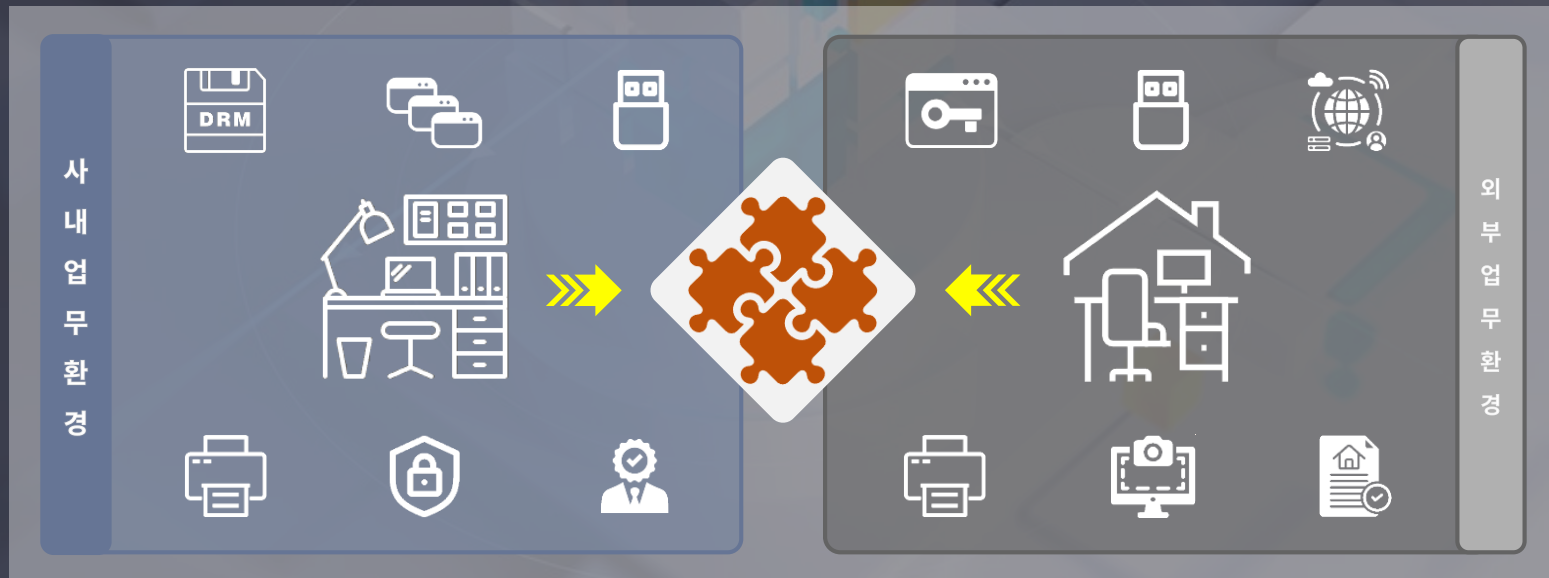
[엔드포인트 통합 보안 솔루션]

사용자를 기준으로 이벤트/행위를 분석할 수 있어야 관제 측면에서 통합을 이점을 살릴 수 있음

보안 솔루션 통합의 조건 #4



In-and-Out



보안 솔루션 통합의 조건 #5



Cost Reduction

개별 PC 보안 취약점 관리는?
회사꺼 말고 개인 노트북도 가능?
사내망 접근 권한 관리는?
USB/화면캡처/프린터까지 통제 가능?
취약점 / 이상징후 발견 시 차단가능?
개인정보 보안성 조치는?
인사 시스템과 연동은?
정책 자동화 가능?
모니터링 / 리포트 / 감사 가능?
중앙 관리 가능?

필요한 포인트 솔루션 10여개

DLP
DRM
NAC
매체제어
PC보안
화면보안
출력보안
개인정보보호

통합
솔루션

구매 및
유지관리
비용



The background is a dark, muted blue-grey color. It features a complex, abstract 3D geometric design. In the center, there's a cluster of light grey and yellow cubes. To the right, a blue cube is visible. Below the central cluster, there's a blue cube with three small blue circles above it. Further down and to the right, there's a yellow cube. The design is composed of various geometric shapes like cubes, spheres, and lines, creating a sense of depth and complexity. The overall aesthetic is modern and technological.

엔드포인트 보안 솔루션 통합 사례

엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A



DLP



네트워크 보안



매체제어



단말기보안



화면보안



출력보안



어플리케이션 보안



중앙관제



다양한 보안 기능의 충분한 검증을 바탕으로 단일 에이전트 엔드포인트 보안 솔루션 적용

엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A

[통합 보안 솔루션 도입 배경]

원격 근무자 보안 수칙	원격근무 환경 운영자/관리자 보안 수칙
전용 공간 확보	통합 인증체계 운영
단말기 보안	원격 근무자 인증보안
프로그램 보안	원격접속 보안
USB 등 외부 미디어 보안	원격접속 자원관리
비밀번호 보안	기업 내부망 모니터링 강화
이메일 보안	비상 대응 절차 운영

[한국인터넷진흥원(KISA) – 비대면 업무환경 도입·운영을 위한 보안 가이드]

엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A

F社
C社
A社

TOCSG
두피에스지

D社
B社

E社

단말기보안

네트워크 보안

데이터 보안

Benchmark Test

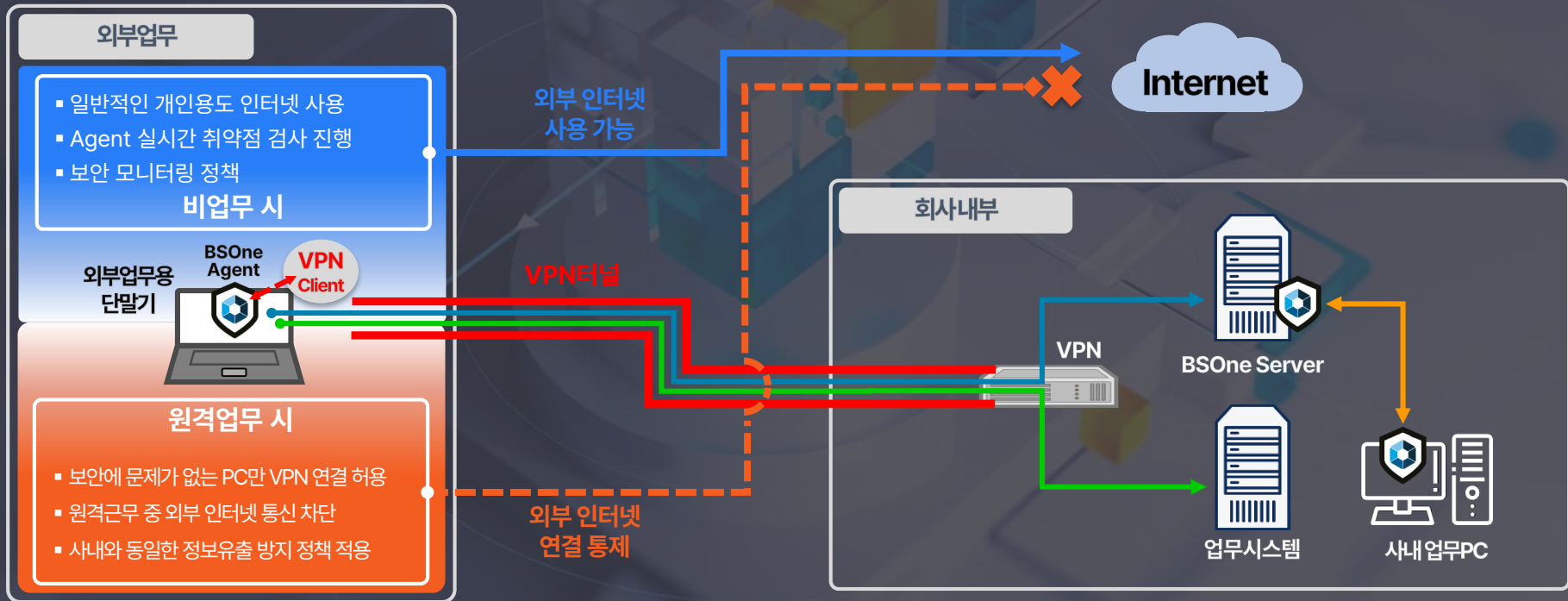
엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A

기능		통합 보안 솔루션 BSOne	원격제어 기반 솔루션 A	NAC 기반 솔루션 B
관리 기능	단말 보안 적용 체크 - OS 버전, 방화벽 버전 체크 - 기타 보안 설정 확인 (화면 보호기 등)	○	○	○
	원격접속 기록 관리	○	○	○
	VPN/화상회의/VDI 연결 등 재택근무 상태 자동 감지	○	X	X
보안 기능	호스트 위변조 방지 및 라우팅 변경 차단	○	X	▲
	정보유출 방지대책적용 - 화면 캡처 방지 - USB 등 매체제어 - 개인정보 등 중요 정보 마스킹(*) 처리 - 내부 전산자료 출력 금지 - 이미지 워터마크 및 스크린 워터마크	○	▲	▲
	전산자료 보호 (외부 단말기 저장 금지)	○	X	X
	업무 중 생성 파일 콘텐츠 수집	○	X	X
	업무 중 외부 인터넷 통신 차단	○	▲	▲
	취약한 프로그램 사용 금지 및 필수 프로그램 사용 관리	○	▲	X
	기본 포트 사용 금지 및 특정 URL 필터/차단	○	▲	▲

엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A



엔드포인트 보안 솔루션 통합 사례 #1

국내 공공기관 A



사용자 불편 최소화



업무용PC 성능 효율



업무 환경 보안성



솔루션
도입/운영 비용



엔드포인트 보안 솔루션 통합 사례 #2

국내 금융기업 B社



라이선스 갱신 이슈가 있는 솔루션 우선 대체 후 정책 마이그레이션을 거쳐 점진적으로 단일 에이전트 통합

엔드포인트 보안 솔루션 통합 사례 #2

국내 금융기업 B社

라이선스 기간이 만료되는 매체제어 솔루션 갱신 이슈

비인가 보조기억매체 통제
USB를 포함한 다양한 보조기억 매체 차단/제어
USB의 읽기/쓰기 등 정책 구분
타 통신 매체 제어 기능
MTP 제어
USB 데이터 케이블 제어
모뎀, 적외선, 블루투스, 무선랜 제어
Badusb 공격 사전 차단
무단 반출 장비에 대한 매체 및 네트워크 제어



USB 제조사별 예외
MTP 장치 제조사별 예외
블루투스 장치 종류별 예외 (예. 주변기기, 헤드셋 등)
블루투스 장치 제조사별 예외

기존 매체제어 솔루션의 기능과 보완이 필요한 보안 기능을 PoC 기간 동안 집중적으로 검증

엔드포인트 보안 솔루션 통합 사례 #2

국내 금융기업 B社



통합 보안 솔루션에 포함된 기존 보안 솔루션 기능을 부서 단위 테스트를 거쳐 점진적으로 전환
DLP/DRM/출력통제를 비롯한 엔드포인트 보안 솔루션 One Agent 통합 실현

엔드포인트 보안 솔루션 통합 사례 #2

국내 금융기업 B社

사내업무환경



외부업무환경



안전하게 업무를 볼 수 있는 사내 보안 환경이 외부에서도 Seamless하게 이어질 수 있는 통합 보안 환경 구성

엔드포인트 보안 솔루션 통합 사례 #3

국내 서비스기업 C社



DLP



DRM



네트워크 보안



매체제어



단말기보안



화면보안



출력보안



개인정보보호



어플리케이션 보안



중앙관제



단일 솔루션을 통해 보안 통합의 조건을 모두 만족하는 엔드포인트 보안 실현!

엔드포인트 보안 솔루션 통합 사례 #3

국내 서비스기업 C社


[엔드포인트 현황 및 보안 담당자의 주요 목표]

1. 개별 보안 솔루션 다수를 운용하기 버거운 낮은 사양의 외부 업무용 단말기
2. 보안 솔루션 운용으로 인한 엔드포인트 성능 저하 방지
3. 사내/외 보안 솔루션 관리 통합

엔드포인트 보안 솔루션 통합 사례 #3

국내 서비스기업 C社



이름	상태	CPU	메모리
>  Unified Security Agent.exe		0.1%	19.3MB

엔드포인트 보안 솔루션 통합 사례 #3

국내 서비스기업 C社



엔드포인트 보안 솔루션 통합 사례 #3

국내 서비스기업 C社



성공적인 엔드포인트 보안 통합



One Agent
One Console



Seamless log



In-and-Out



Cost Reduction

성공적인 엔드포인트 보안 통합



DLP



DRM



네트워크 보안



메일제어



단말기보안



화면보안



출력보안



개인정보보호



어플리케이션 보안



중앙관제



현 IT보안 인프라 현황 분석을 바탕으로 점진적인 대체/통합을 통해 성공적인 통합 실현!

The background is a dark, muted blue-grey color. It features a complex, abstract 3D geometric design. In the center, there is a cluster of cubes in various shades of blue, teal, and yellow. Some cubes are stacked, while others are floating or connected by thin, light blue lines. A prominent circular line with arrows at its ends encircles the central cube cluster. Other geometric shapes, including lines and small cubes, are scattered across the background, creating a sense of depth and movement. The overall aesthetic is modern and technological.

감사합니다.