

Zero Trust, AI and SASE: 그래서 Cato는?

(싱글 컨텍스트로 누리는 보안)

김지민 수석
Sales Engineer / APJ



최근 보안 침해 사고 동향 - 2024년

피싱...파밍...개인정보 유출...랜섬웨어...

2023년 랜섬웨어 지불 비용, 1조 5천억원에 달했다

HOME > 경제 > 산업

[기획] 잇따른 개인정보 유출 사례... 실혹서...

김성지 기자 | 승인 2024.07.26

모바일 청첩장 눌렀다가 개인정보 유출... 7천만원 대출 피해

2024년 3월 랜섬웨어 공격 사례 집계해보니... 록비트와 플레이로 가장 큰 피해

입력: 최근 국내 제조·건설·교육 기관 타깃 안다리엘 해킹그룹 APT 공격 확인돼



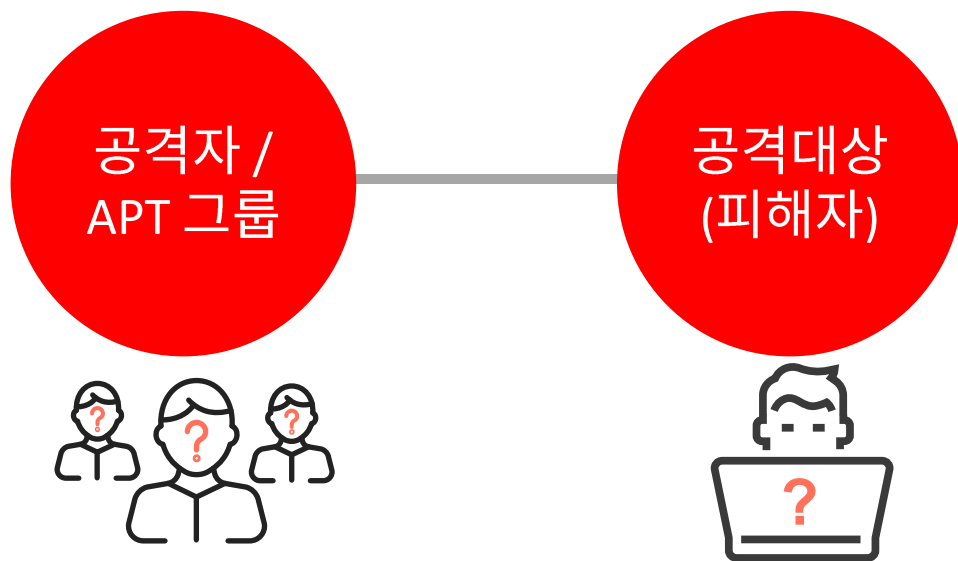
최근 국내 제조·건설·교육 기관 타깃 안다리엘 해킹그룹 APT 공격 확인돼

길민권 기자 | 승인 2024.05.18 15:55

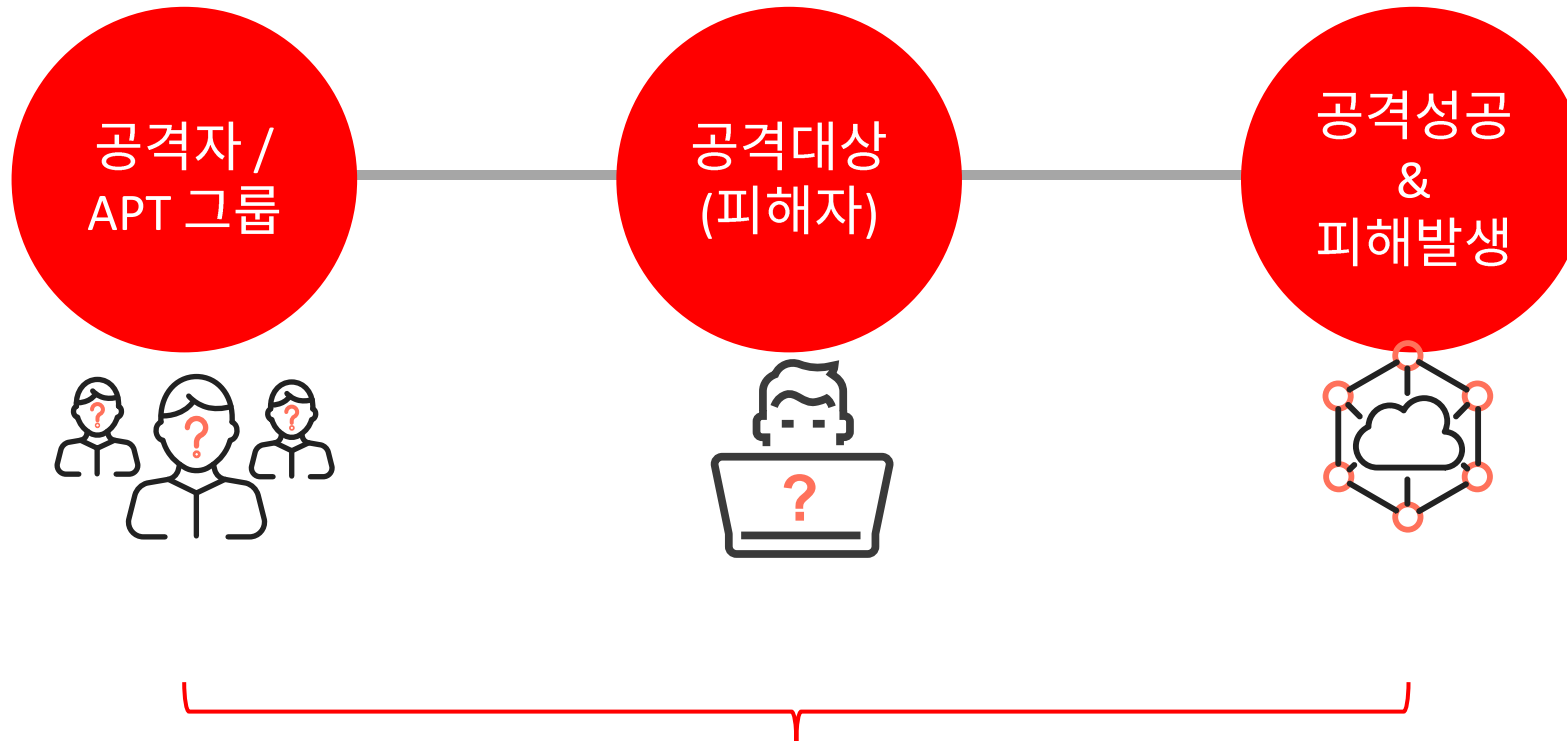
일반적인 보안위협 양상



일반적인 보안위협 양상



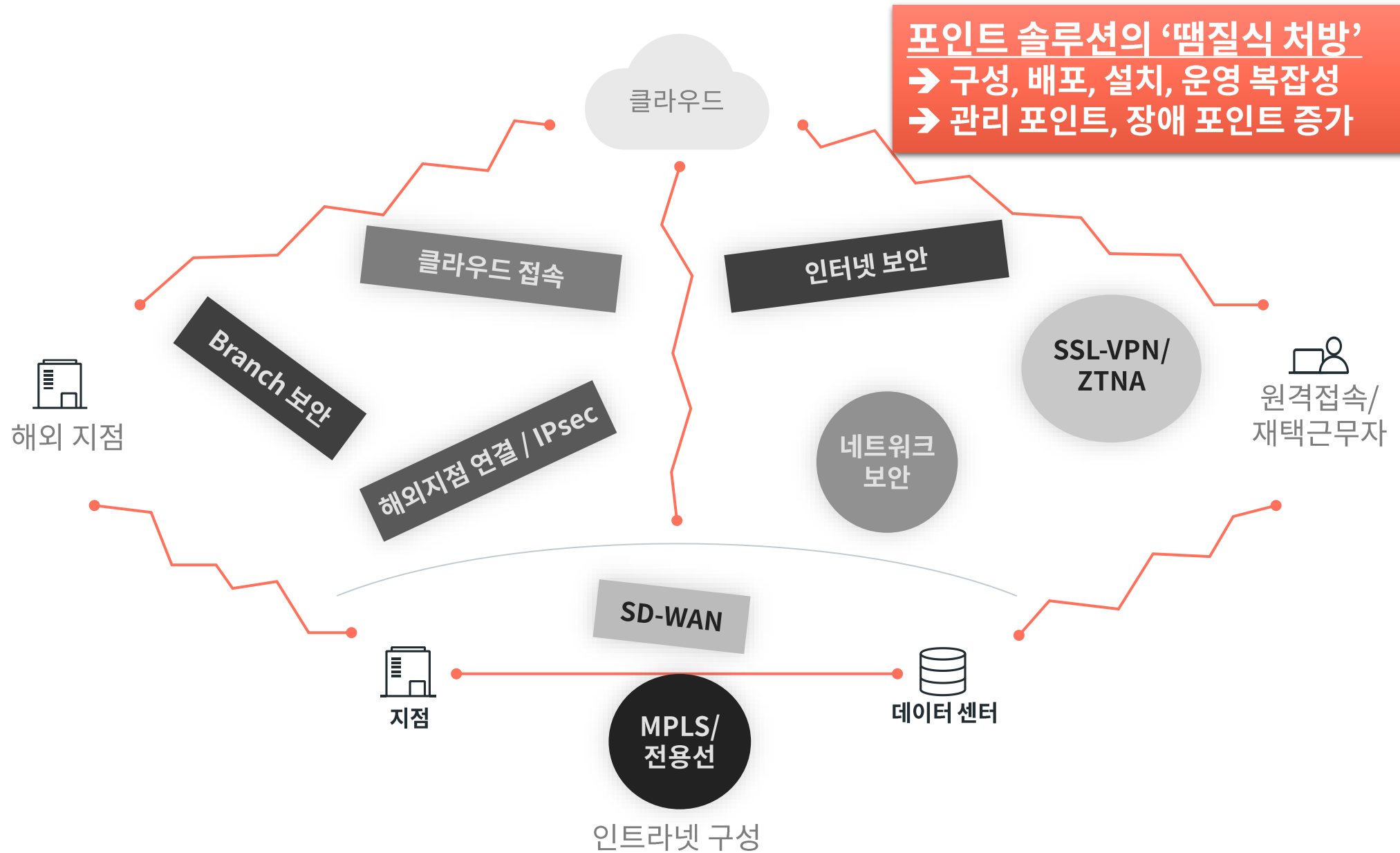
일반적인 보안위협 양상



다양한 공격자들이 존재하는 한
우리는 지속적인 위협에 노출되어 있으며
어디선가 피해가 발생하고 있음

비즈니스 요구 확장 = 네트워크 보안 대상 영역의 확장

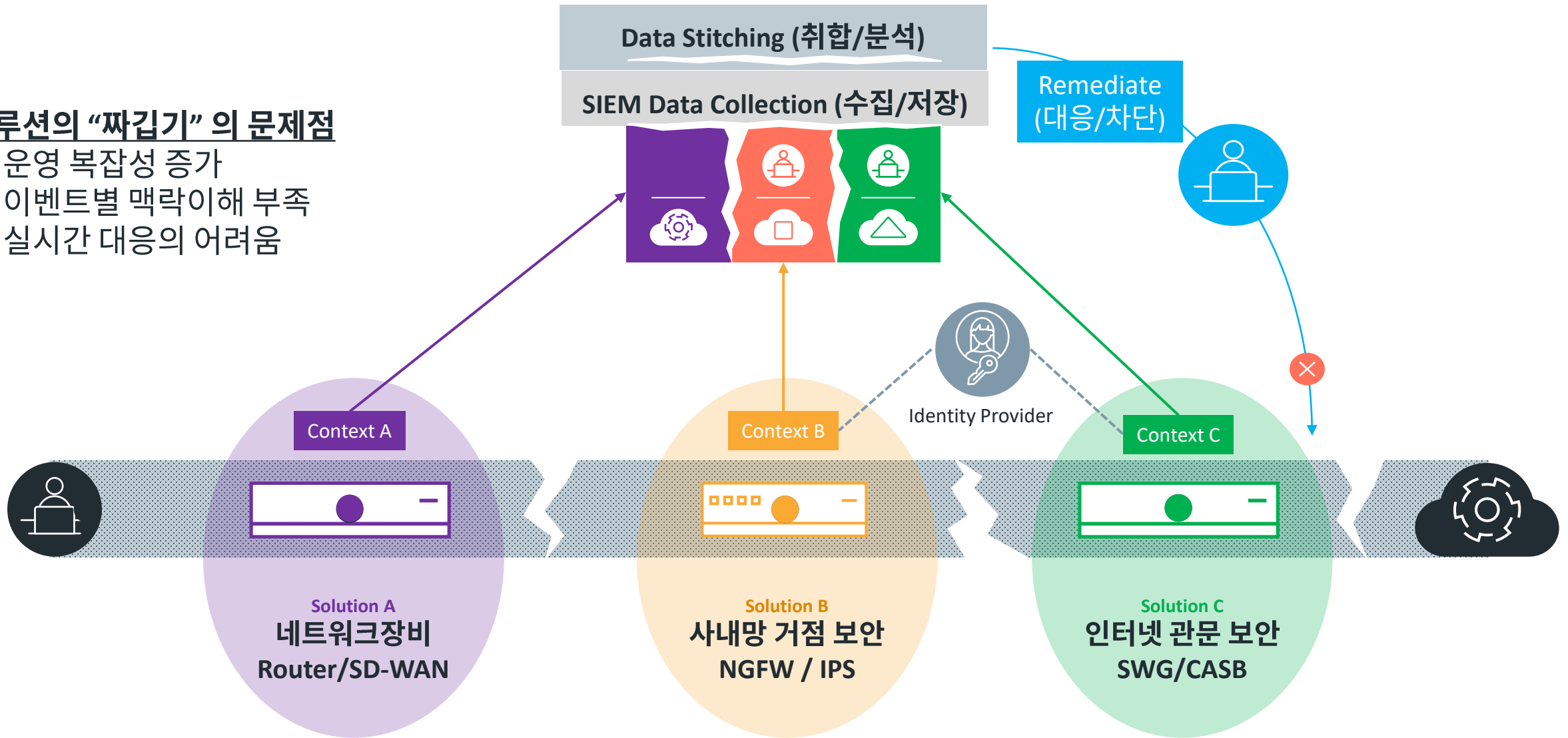
정보보안의
현실



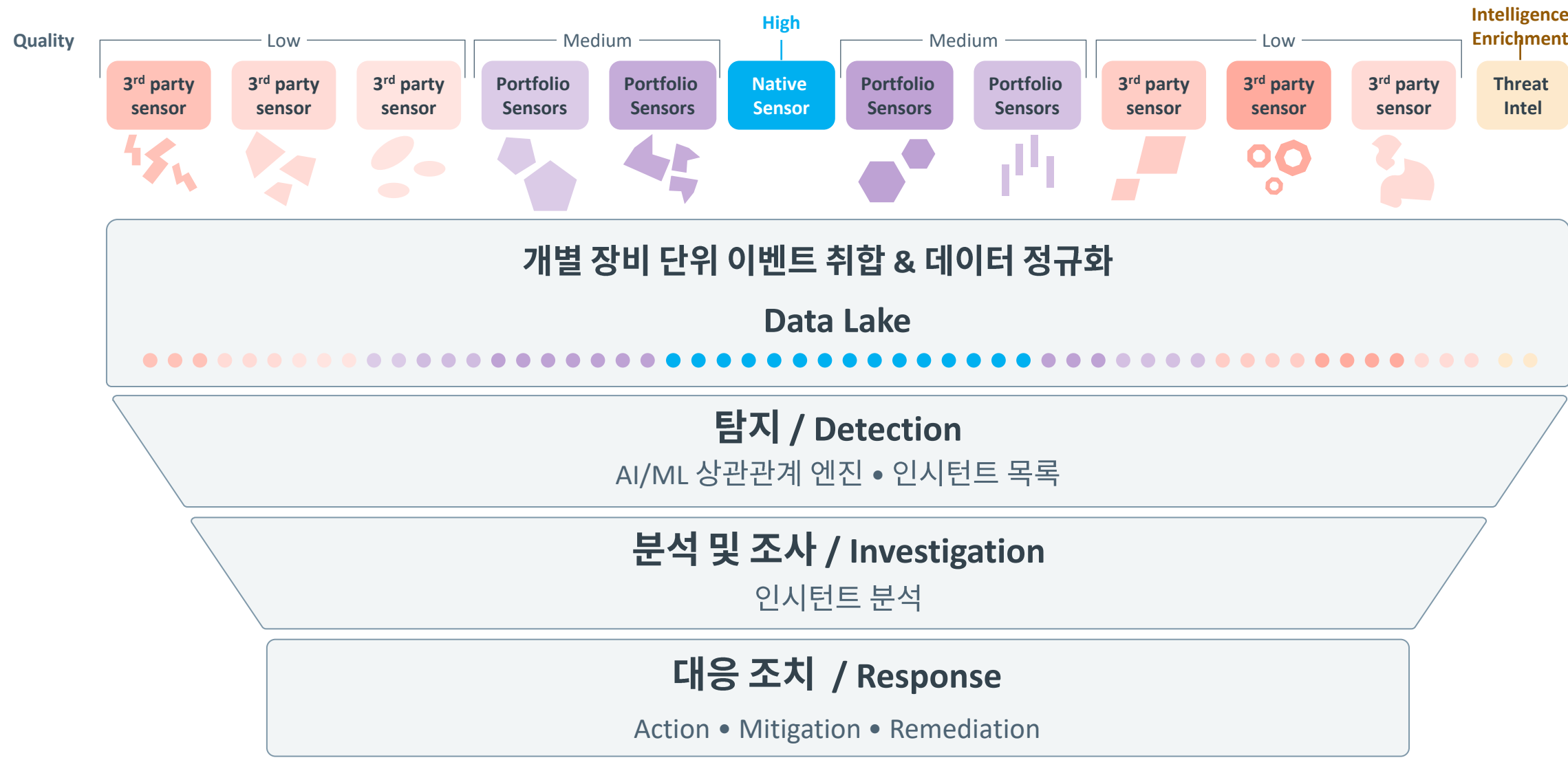
“Single Vendor SASE” ≠ “Single Pass Architecture”

솔루션의 “짜깁기” 의 문제점

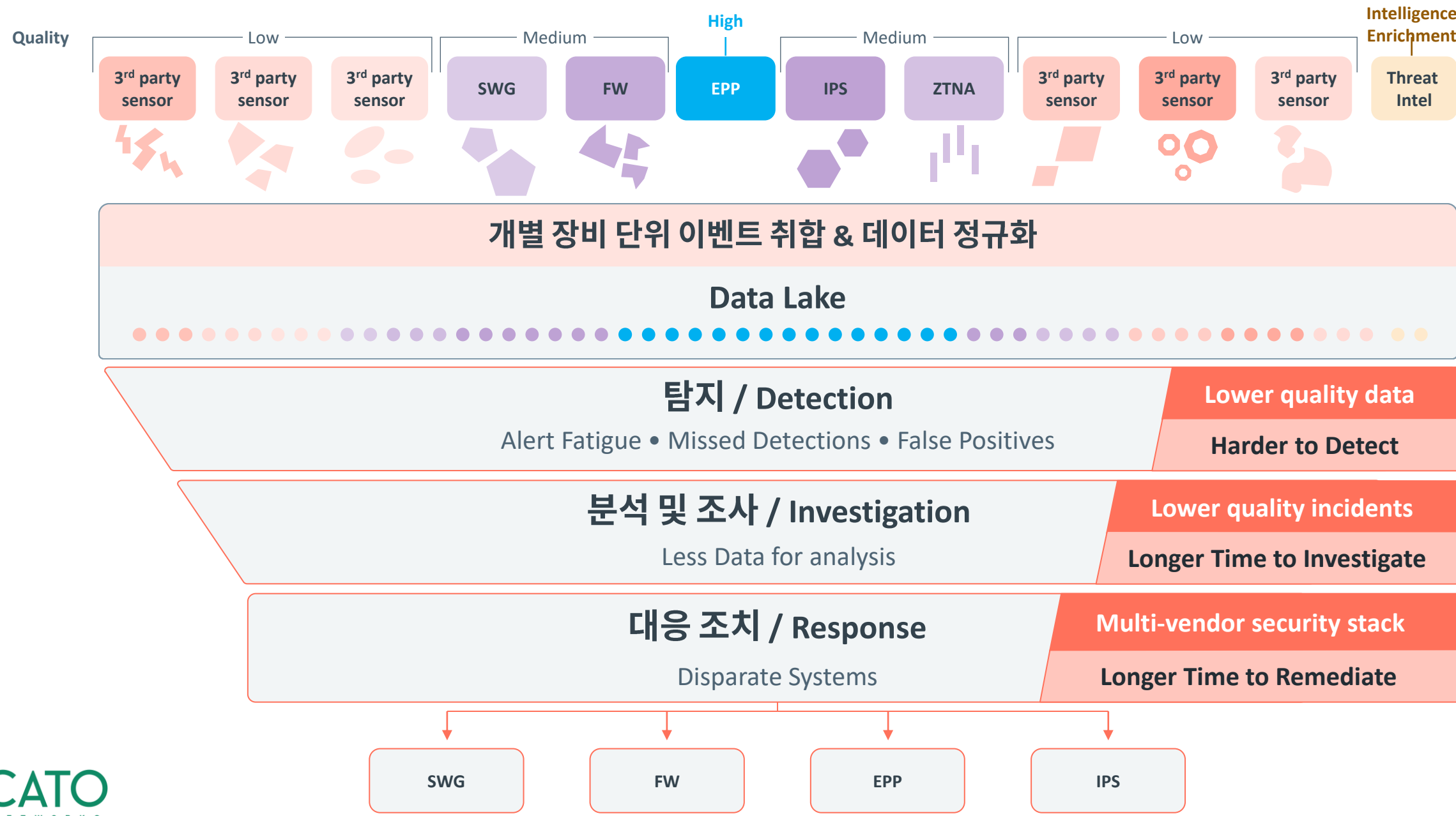
- 운영 복잡성 증가
- 이벤트별 맥락이해 부족
- 실시간 대응의 어려움



전형적인 XDR 솔루션의 구성



대부분의 XDR 운영 현실 (EPP등 일부 영역만 Native Sensor 활용)



정보보안의
현실



유연하지 않은
접근 보안 정책

접근 보안 정책



제한적인
보안 가시성 및
데이터 분석 방안

데이터 분석 방안
보안 가시성



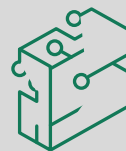
비효율적인
위협 탐지 및 침해
대응 체계

대응 체계
위협 탐지 및 침해

What
If.....



Identity-기반의
일관적인 Universal
ZTNA



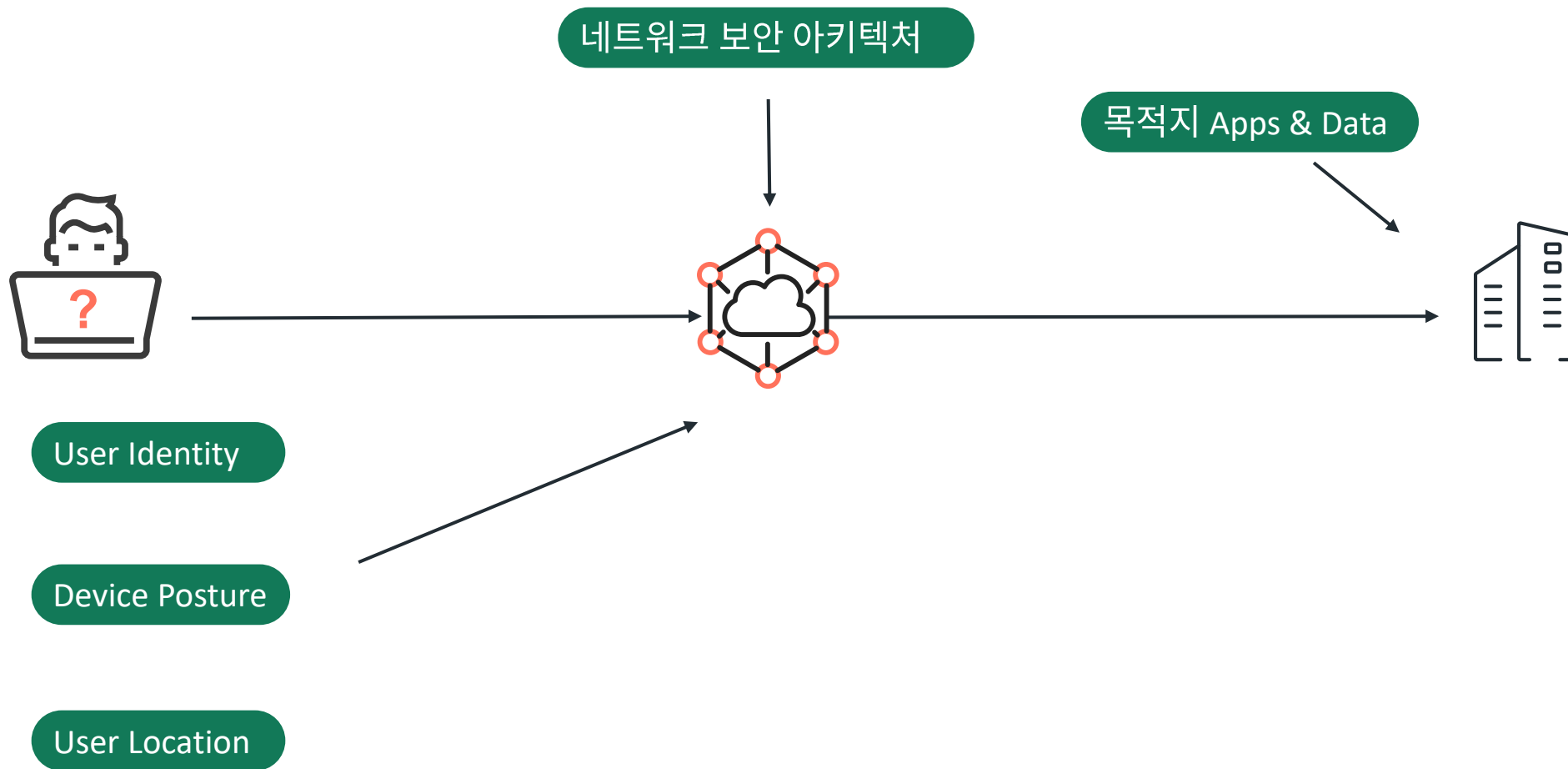
능동적인 AI 기반의
위협예방 체계



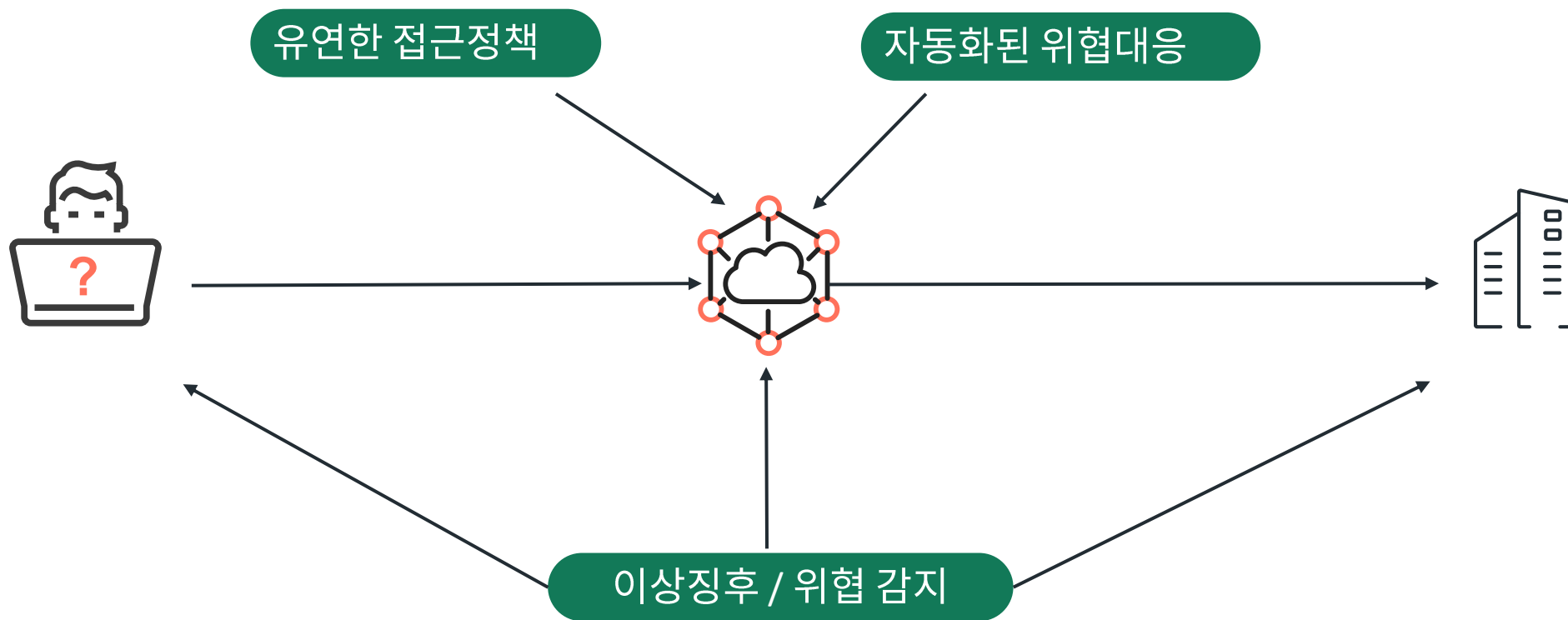
SASE-기반의
일원화된
탐지&대응 체계

Zero
Trust

사용자 접속시점
➔ 사용자 보안성 평가 실행
(아이덴티티, 단말 보안태세, 사용자 환경)



인텔리전트한 접근제어 & 위협 탐지





Zero Trust, AI and SASE

그래서 Cato는...어떻게?

AI +
Zero
Trust

ZTNA 를 위한 다양한 접속 형태 지원
“Security that follows the user”

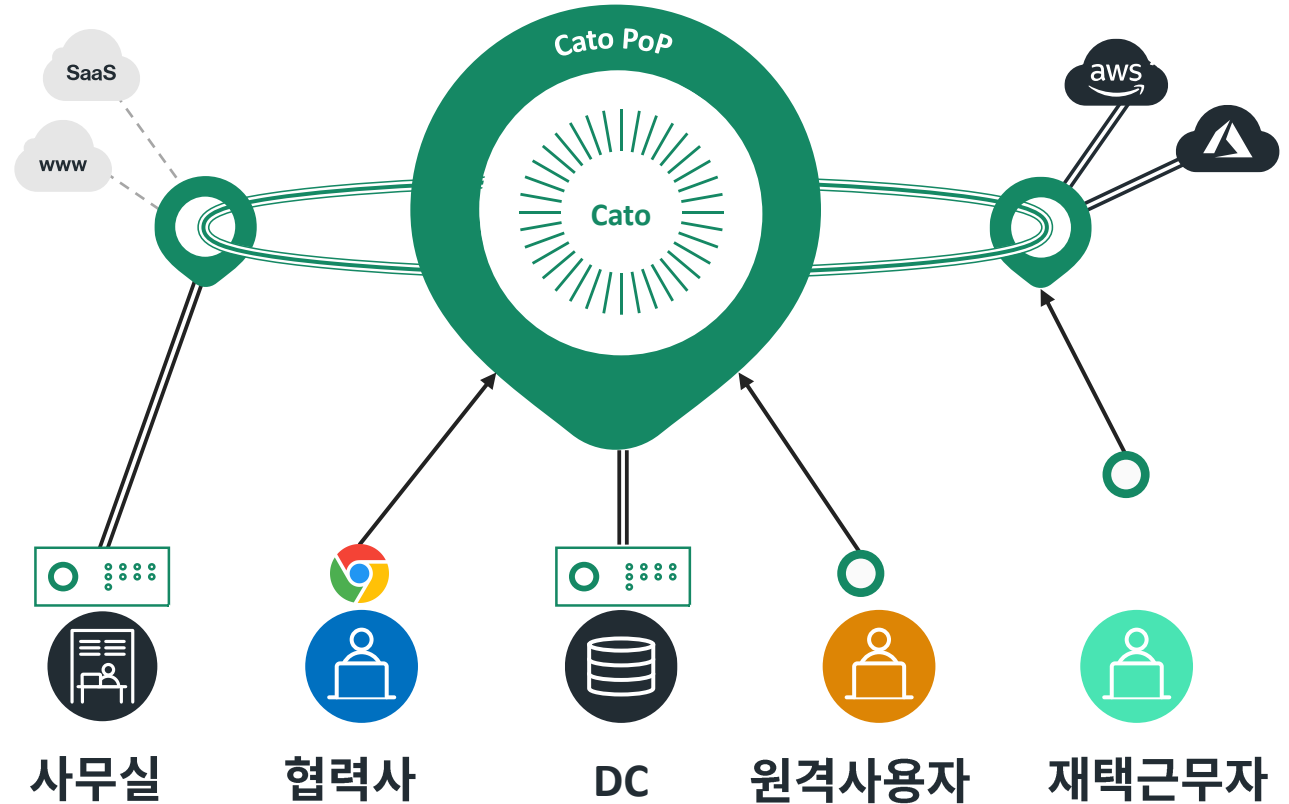
일관적인 접근 정책

- 사용자 아이덴티티 기반의 정책 구성
- 접속지역, 사용자 단말과 무관
- 전세계 팝과 실시간 정책 동기화

제로 트러스트: “Trust but Verify”

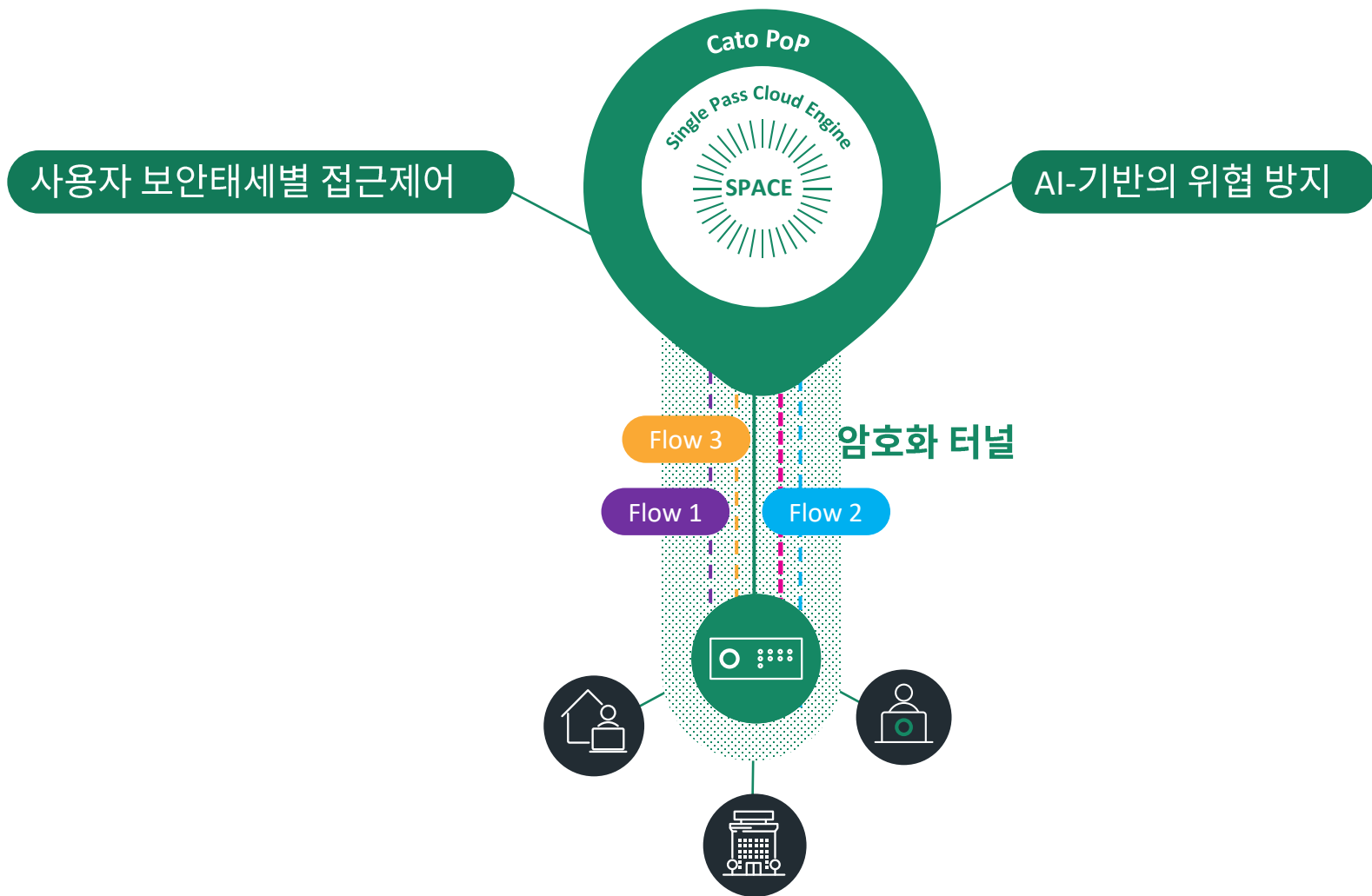
사용자 단말의 보안태세수준에 따른 차등 권한 부여

- 위협 예방 (FWaaS, SWG, IPS, AM)
- 민감 정보 보호 (DLP)
- 위험도에 따른 어플리케이션 접근 권한 제어 (CASB)



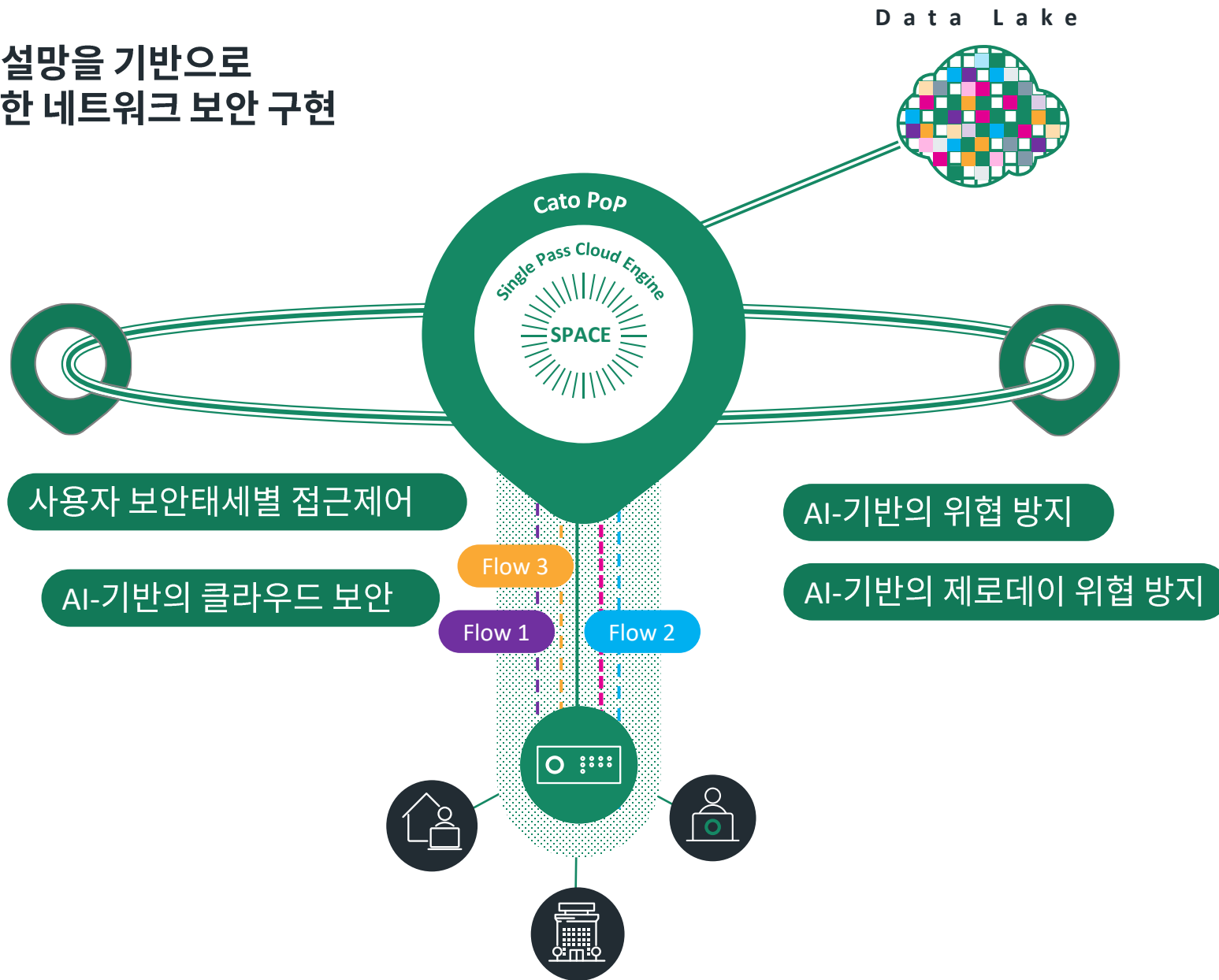
SASE +
AI +
Zero
Trust

맥락 (Context) 기반의 실시간 보안 제공 “Context is King”



SASE +
AI +
Zero
Trust

글로벌 사설망을 기반으로
AI를 활용한 네트워크 보안 구현



AI-Powered SASE 플랫폼: Cato 서비스내 다양한 AI 활용 사례

Security

실시간 위협 방지 및 오프라인
탐지를 위해 AI/ML 분석 활용

SASE Copilot

Cato 포털상 자연어를 이용한
통합이벤트 조회, 보안 위협 검토등
일상적인 관리자 업무 지원

Networking

사용자 실 트래픽의
"메타데이터"를 추적하여 글로벌
트래픽 동향 및 특이사항 감지

Platform

고객사 관리자 플랫폼 경험 개선을
위한 백엔드 서비스 강화
생성형 AI 기반의 사용성 제공

Support

AI 툴을 활용한 KB문서포털 및
장애접수 플랫폼에 통합
고객 서포트 지원 강화

AI 활용예: 실시간 위협 방지 모델

피싱 위협: 사이버 스쿼팅



- Faceb00k.com: 숫자 '0'
- Faceb◦◦k.com: 한글의 '이응'
- Facebook.com: 키릴언어 'a'
- microsoft.com: 짧은 간격의 N N

도메인관련 위협정보 인텔리전스
+
접속대상지에 대한 유명도 (평판조회)등

실시간 AI 분석으로 접근 승인 여부 판단

AI 활용예: 실시간 위협 방지 모델

봇넷 감염 / DGA 탐지 사례

qalus.com	naqodur.com
mucac.com	pocakaqu.com
sanaju.com	qunadap.com
jurokotu.com	womohu.com
kuqotaj.com	wuqah.com
lufacam.com	dagaju.com
bunafo.com	bosojojo.com
bunupoj.com	dubocosos.com
cajato.com	fupoj.com

특정 도메인 접속 증가



해당 도메인간 상관관계 유추



평판조회 및 유명도 비교



동일한 도메인 업체 등록



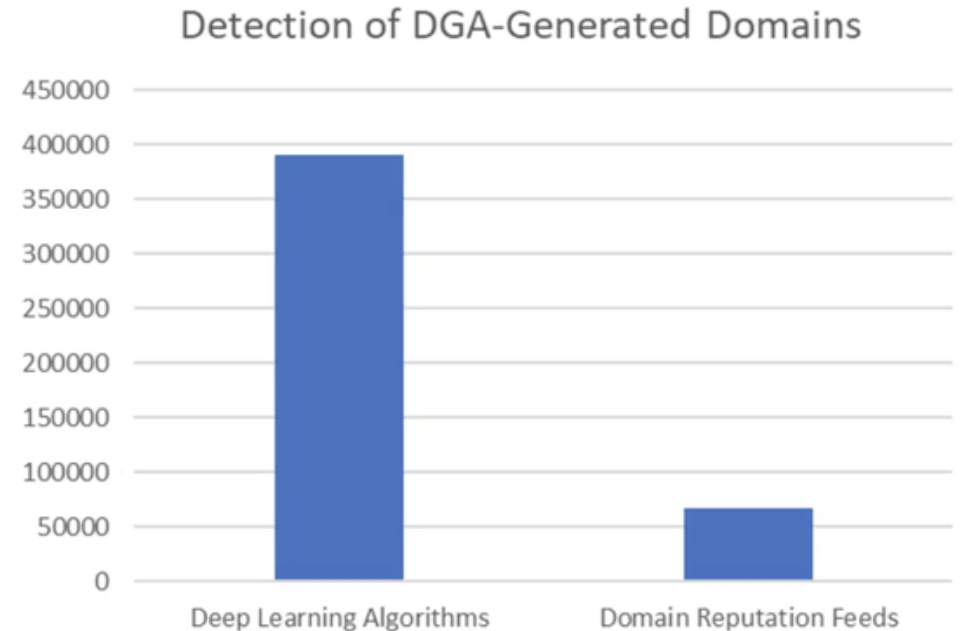
DGA 기반의 멀웨어 감염된
트래픽 패턴의 유사성 확인

AI 활용예: 실시간 위협 방지 모델

- Cato 글로벌 백본내 처리된 All 트래픽의 메타데이터 수집
- 고객별 실 트래픽에 대한 실시간 보안 검사 수행
- 이상 트래픽 감지 시 예방적 차단 및 위협 사냥 절차 실행
- **일반 인텔리전스 피드 검사 대비 탐지율 향상 (6배+)**
 - a) Cato SASE 보안 플랫폼에서 AI 기법을 활용해 선제적으로 차단한 DGA 관련 트래픽중
 - b) 250+ 개 이상의 위협 인텔리전스 피드에 등재된 (이미 알려진) 악성 목적지는 단지 15% 에 불과
 - ➔ 인텔리전스 피드 의존시 위협정보 업데이트의 지연시간, 상이한 신뢰성에 따른 필연적인 보안 사각지대 존재

Real-time Deep Learning Yields 6X Improvement in Threat Detection

Cato Research Labs routinely observes tens of millions of network connection attempts to DGA domains from across the 1700+ enterprises using the Cato SASE Cloud. For example, of the 457,220 network connection attempts to DGA domains made in a sample period, only 66,675 (15 percent) were listed in the 250+ threat intelligence feeds consumed by Cato. By contrast, Cato algorithms identified the rest, over 390,000 additional DGA domains, a nearly six-fold improvement.



Product Catalogs (위협정보 / 어플리케이션 정보 생성 자동화)

Threats

Threat Catalog				
Name	Signature	Mitre Technique	Engine	Status
<input type="text" value="cve"/>	<input type="text" value="Search signature"/>	<input type="text" value="Select Mitre Technique"/>	<input type="text" value="IPS"/>	<input type="text" value="All"/>
Name	Description	Threat Name/Signature ID	Engine	
CVE-2022-24218 - eliteCMS Arbitrary File Deletion	The eliteCMS v1.0 /admin/delete_image.php has a vulnerability that permits attackers to delete any file of their choosing.	cid_cve_2022_24218	IPS	
CVE-2014-7169 - GNU Bourne-Again Shell (Bash) Arbitrary Code Execution	CVE-2014-7169 is a vulnerability in GNU Bash that allows remote attackers to write to files or have other unknown impacts when malformed function definitions are used in environment variables. This vulnerability is a result of an incomplete fix for CVE-2014-6271 and can occur in various situations such as with OpenSSH sshd, Apache HTTP Server, and DHCP clients.	cid_heur_shellshock	IPS	
CVE-2018-0101-1 Cisco adaptive security appliance remote code execution and denial of service vulnerability	CVE-2018-0101 is a vulnerability in Cisco Adaptive Security Appliance (ASA) Software. It allows an unauthenticated, remote attacker to cause a system reload or execute code on affected devices. The vulnerability is caused by an attempt to double free a region of memory when the webvpn feature is enabled.	cid_cve_2018-0101_1	IPS	
CVE-2018-6389-1 Wordpress parameter resource consumption remote dos	CVE-2018-6389 is a vulnerability in WordPress 4.9.2 and earlier versions that allows unauthenticated attackers to create a denial of service attack by repeatedly requesting a large number of JavaScript files from wp-includes/script-loader.php. This would cause a high amount of resource usage.	cid_cve_2018_6389_1	IPS	
CVE-2018-6389-2 Wordpress parameter resource consumption remote dos	CVE-2018-6389 is a vulnerability in WordPress that allows unauthenticated attackers to cause a denial of service (resource consumption) by making multiple requests to a long list of JavaScript files. This can cause the server to become overwhelmed and unable to respond to legitimate requests.	cid_cve_2018_6389_2	IPS	
CVE-2017-0199 Microsoft office/wordpad remote code execution vulnerability	CVE-2017-0199 is a vulnerability in Microsoft Office and Windows that allows remote attackers to execute arbitrary code. This is done by exploiting a crafted document and exploiting the Windows API. It affects Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, 2016, Windows Vista SP2, Server 2008 SP2, Windows 7 SP1 and Windows 8.1.	> cid_cve_2017_0199 (+1)	IPS	
CVE-2017-5638 Apache struts jakarta multipart parser ognl injection	CVE-2017-5638 is a vulnerability in Apache Struts 2 that allowed attackers to execute arbitrary commands via a crafted HTTP header. This vulnerability was exploited in the wild in March 2017 and was caused by incorrect exception handling and error-message generation during file-upload attempts.	> cid_cve_2017_5638 (+1)	IPS	

Applications

Spotify is a commercial music streaming service that provides restricted digital content from a range of record labels and artists.

Media StreamsCloud Application3

GeneralAdd To Sanctioned Apps

Spotify is a commercial music streaming service that provides restricted digital content from a range of record labels and artists. Users can browse through the interface by artist, album, genre, playlist, record label, and direct searches. It also enables individuals to create, share, and edit playlists with other users. If users want recommendations, they can integrate their system with Last.fm, an application that provides music recommendations based on listening history. The radio feature installed in Spotify creates random playlists for its users that are related to preferred artists. Spotify is available for mobile device platforms such as Android, Blackberry, Boxee, iOS, Linux, MeeGo, Squeezebox, Windows mobile, and more.

Compliance

ISAE 3402SOC 1

PCI-DSSSOC 2

ISO 27001SOC 3

SOX

HIPAA

Security

MFASSO

Encryption At RestTrusted Certificates

Audit TrailHTTP Security Headers

RBACTLS Enforcement

Remember Passwords

Stockholm, Stockholms Lan, Sweden

http://www.spotify.com

5001-10000

IPO

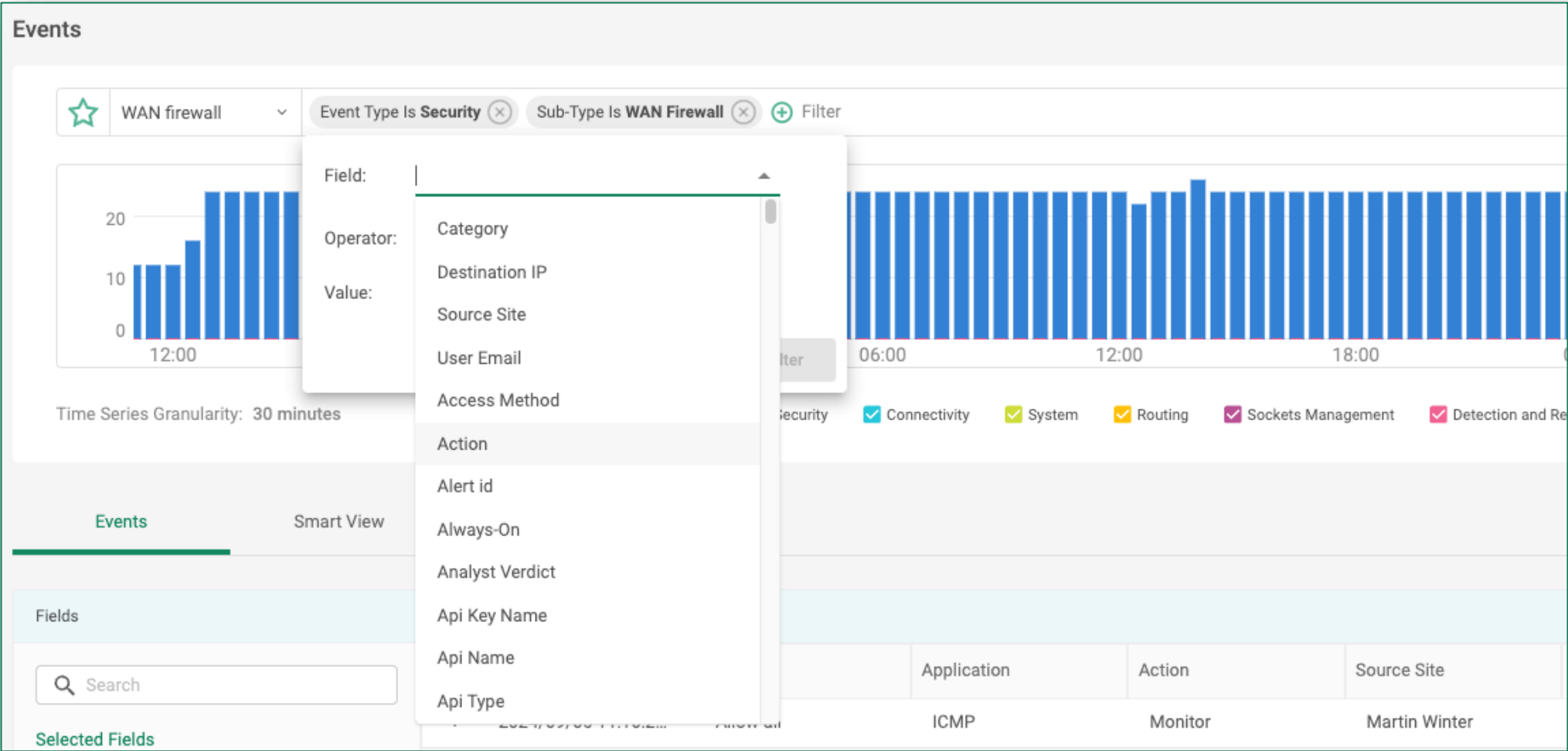
<https://support.catonetworks.com/hc/en-us/articles/10055007301149-Using-the-Threat-Catalog>

<https://www.catonetworks.com/blog/cato-application-catalog-how-we-supercharged-application-categorization-with-ai-ml/>

생성형 AI: 자연어기반 이벤트 로그 검색

Current behavior

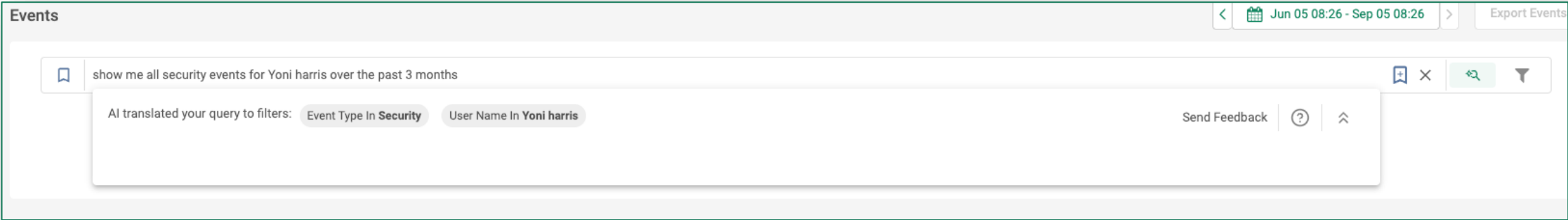
Admin can query and retrieve data in 'Events' page only by using the **current filter bar**.



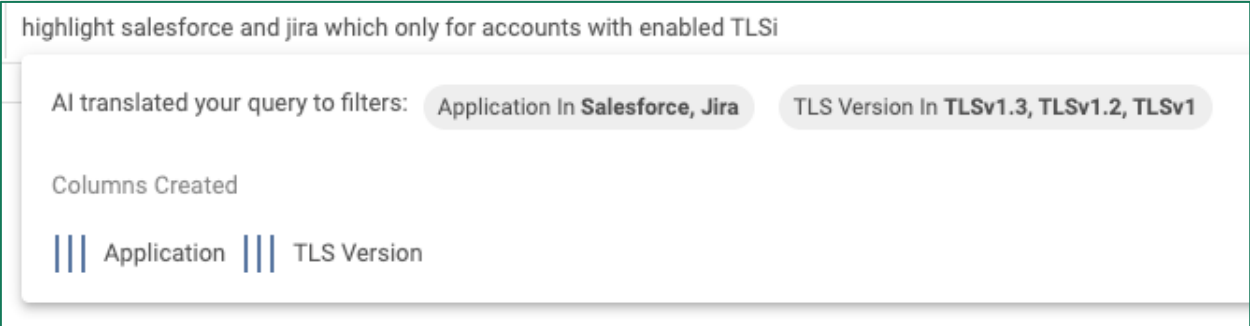
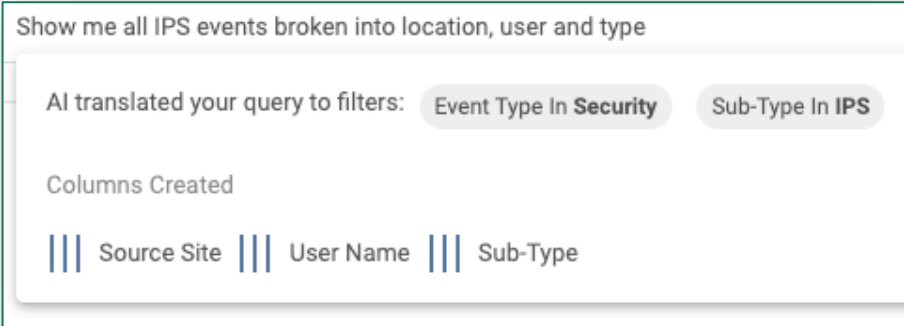
Natural Language Search (Gen-AI in CMA)

New solution of AI-based search within CMA

The new AI-powered search component offers built-in free-text search functionality, and a dual-mode interface for side-by-side work.



Real-world examples



Gen-AI in CMA

Already in CMA:

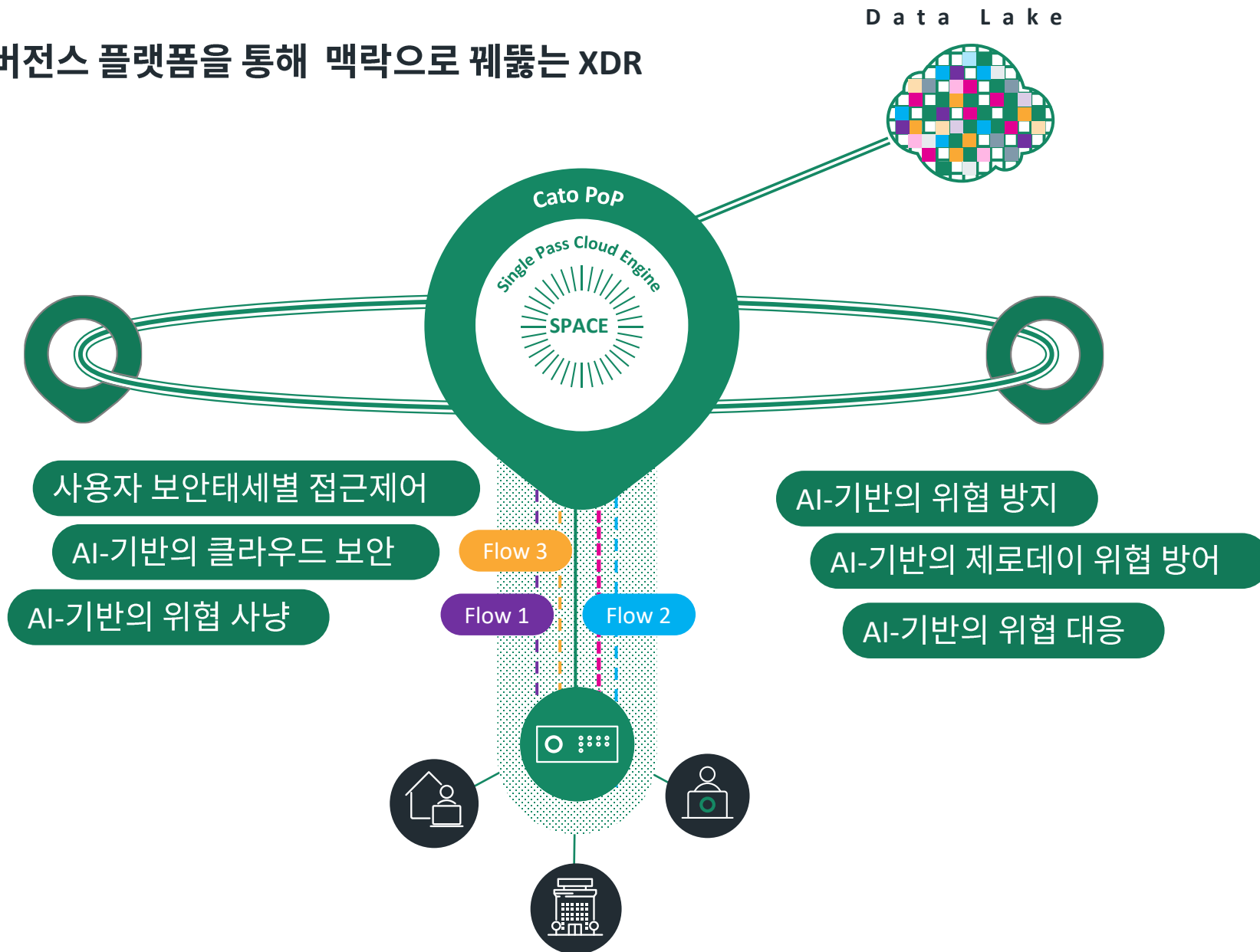
1. XDR Storyteller - AI-based summary of Cato stories
2. Localization – CMA is translated into 9 languages including Japanese, French, Spanish and more

Coming Soon:

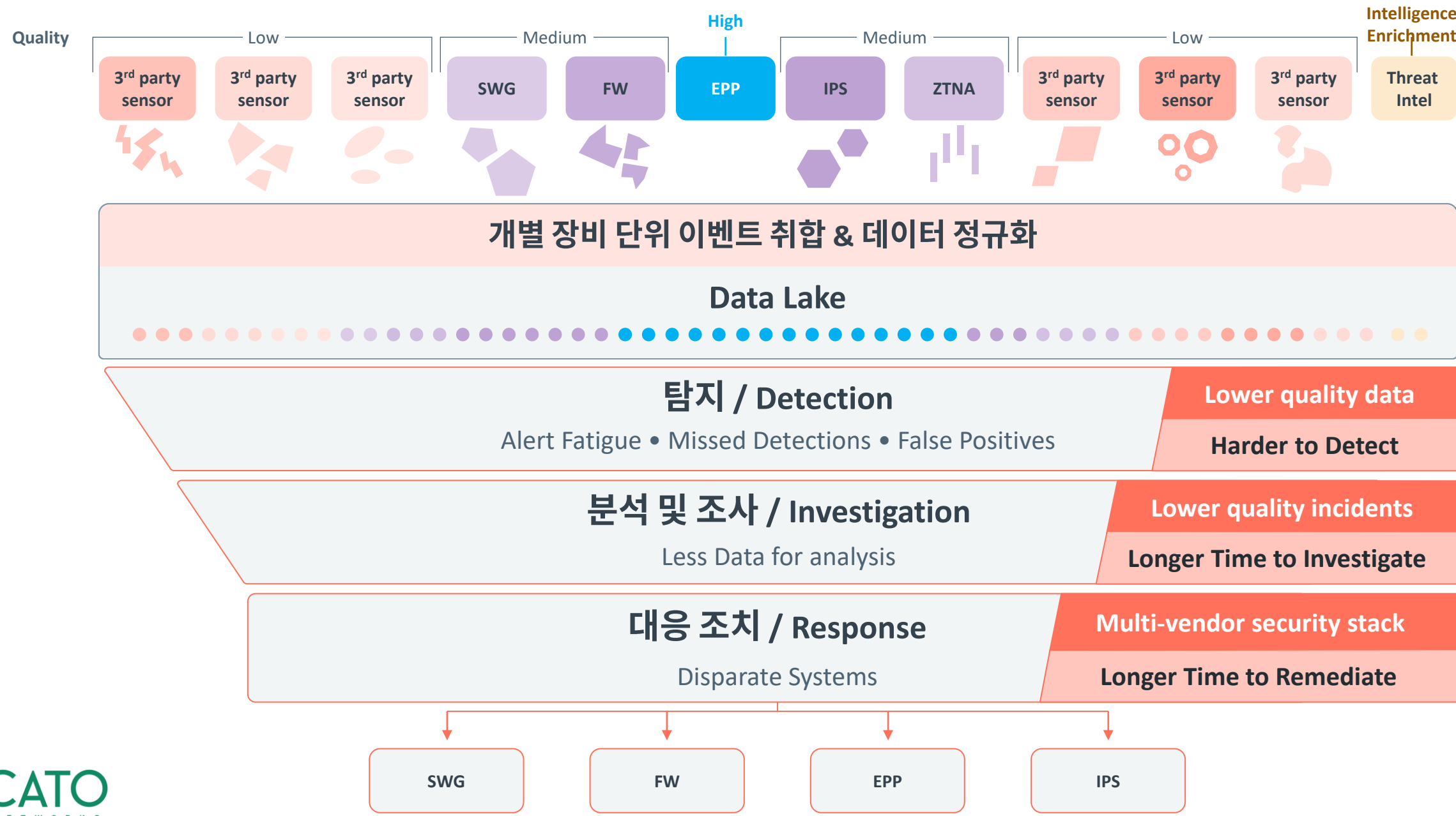
1. KB Assistant – answer How-To questions
2. API Generator – code based on Cato API public schema
3. Policy optimizers – integrating AI capabilities into our policy engine

SASE +
AI +
Zero
Trust

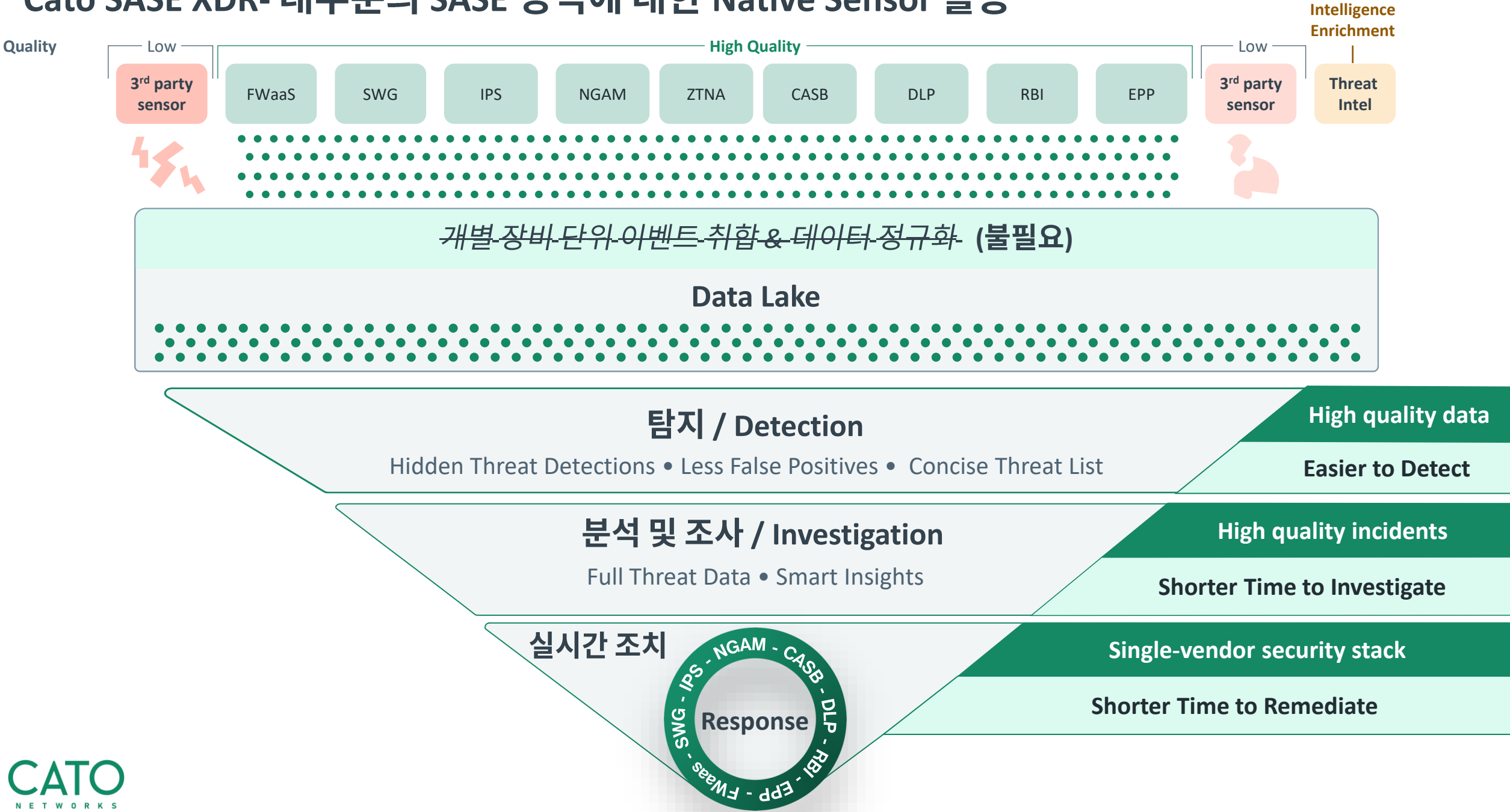
SASE 컨버전스 플랫폼을 통해 맥락으로 꿰뚫는 XDR



대부분의 XDR 운영 현실 (EPP등 일부 영역만 Native Sensor 활용)



Cato SASE XDR- 대부분의 SASE 영역에 대한 Native Sensor 활용



Mitigate
Risk

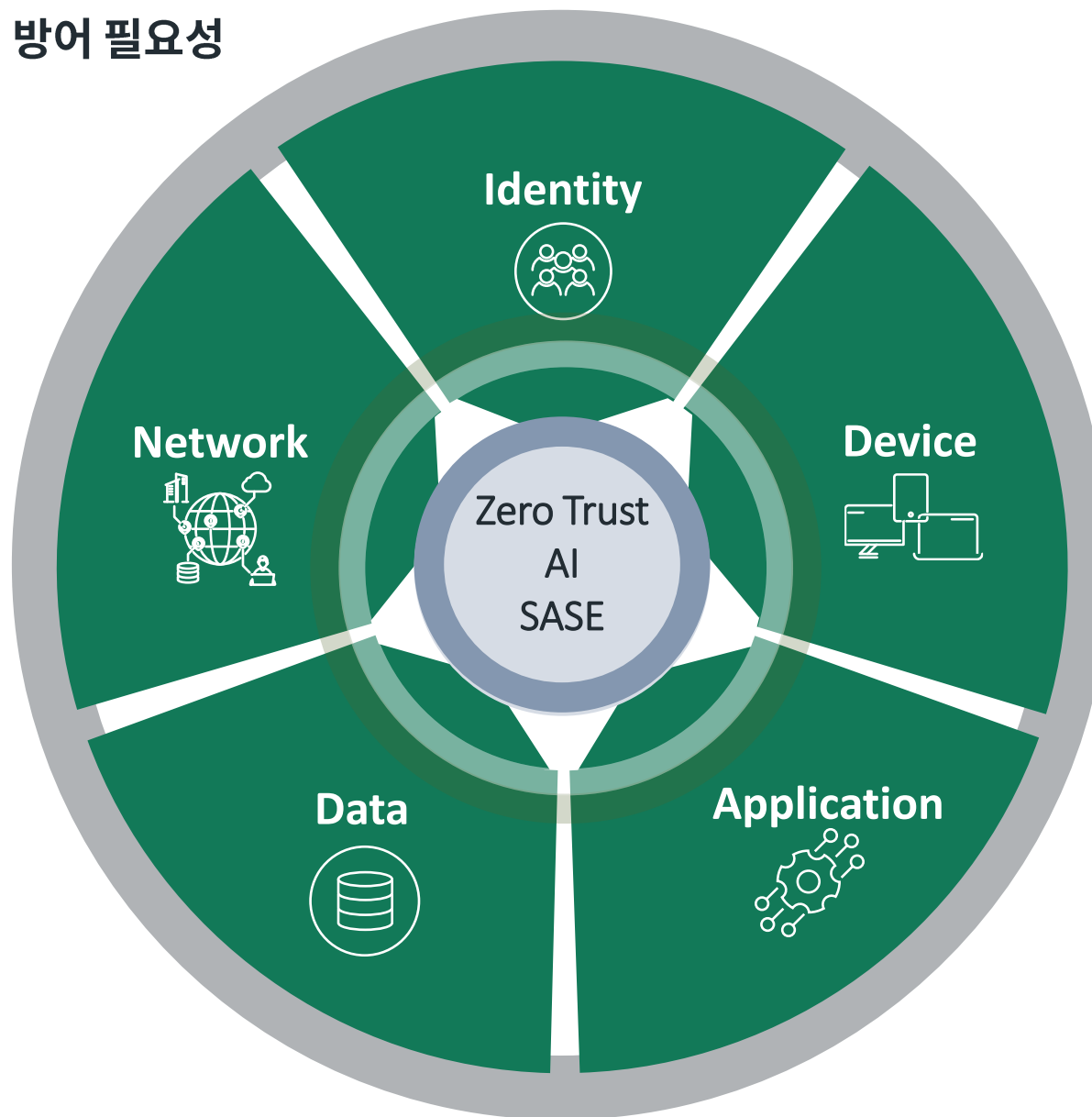
SASE + AI + Zero Trust



- **Real-Time Assessment** – Continuous risk evaluation & real-time adaptation
- **Behavioral Analytics** – Learn & adapt according to risk profile
- **Anomaly Detection** – Enforce appropriate access policies everywhere
- **Automate Threat Response** – Swiftly neutralize threats

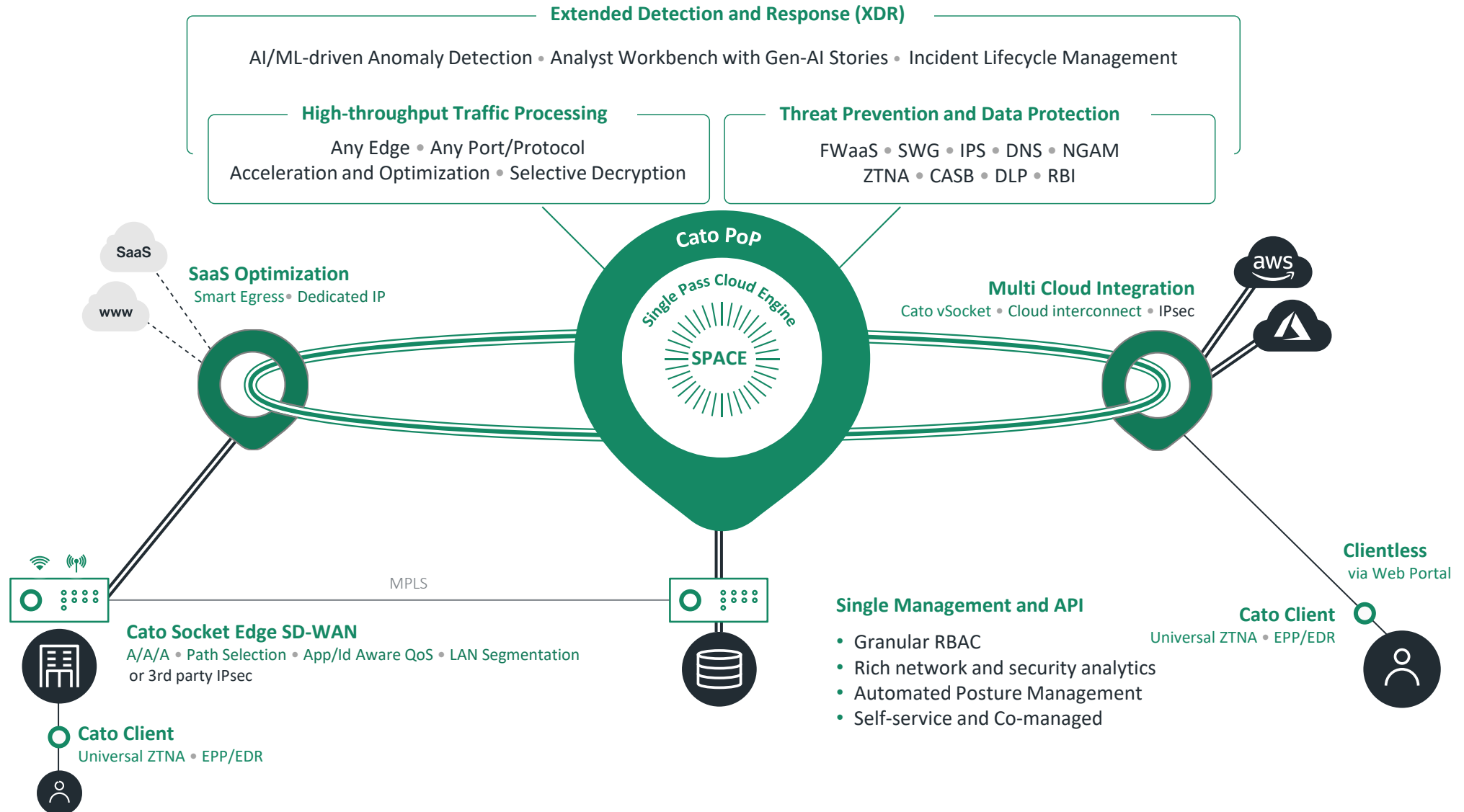
360-
Degree
Security

전방위적 위협 방어 필요성



AI-Driven 보안을 제공하는 전방위적 위협 방어 체계

The World's First SASE
platform



● — 강력한 보안의 바탕



Universal ZTNA



Dynamic AI-Driven
Threat Prevention



SASE-based
Detection &
Response

CATO

N E T W O R K S

We are SASE