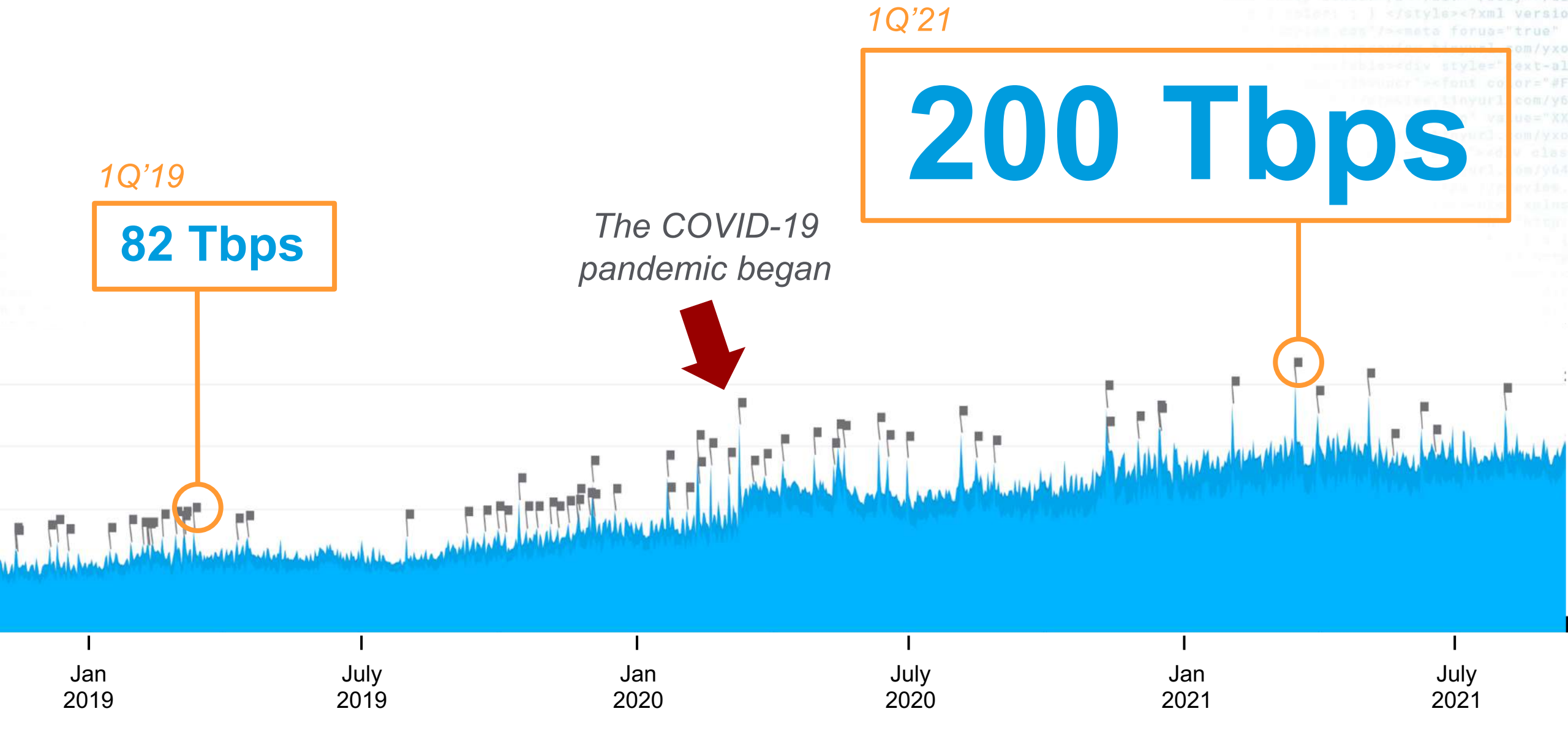
계정 탈취 (ATO) 생태계의 이해와 방어

Akamai Technologies, Korea
기술 영업팀

한준형 (Chun Han)

Traffic Growth on Akamai



이 세상은 온라인입니다...그리고 트래픽은 급증하고 있습니다.

1분기 매일 피크는 100 Tbps 이상

1분기 평균 피크는143 Tbps

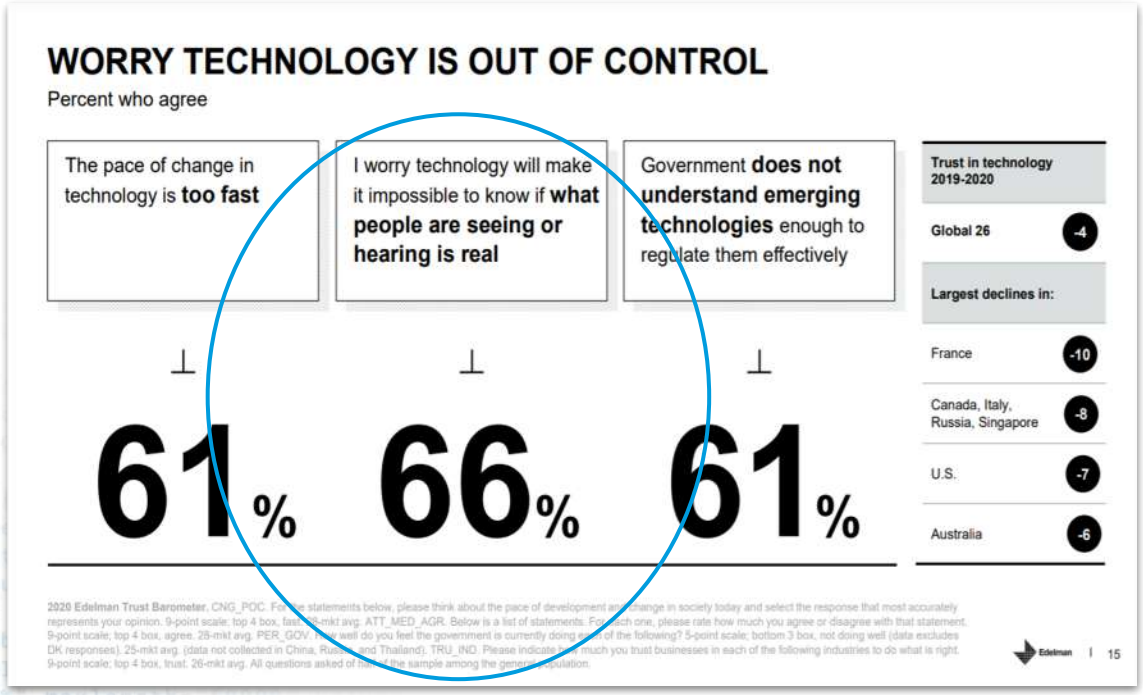
이는 작년 1분기 대비 47% 높은 수치입니다.

달 별 Y/Y 차이

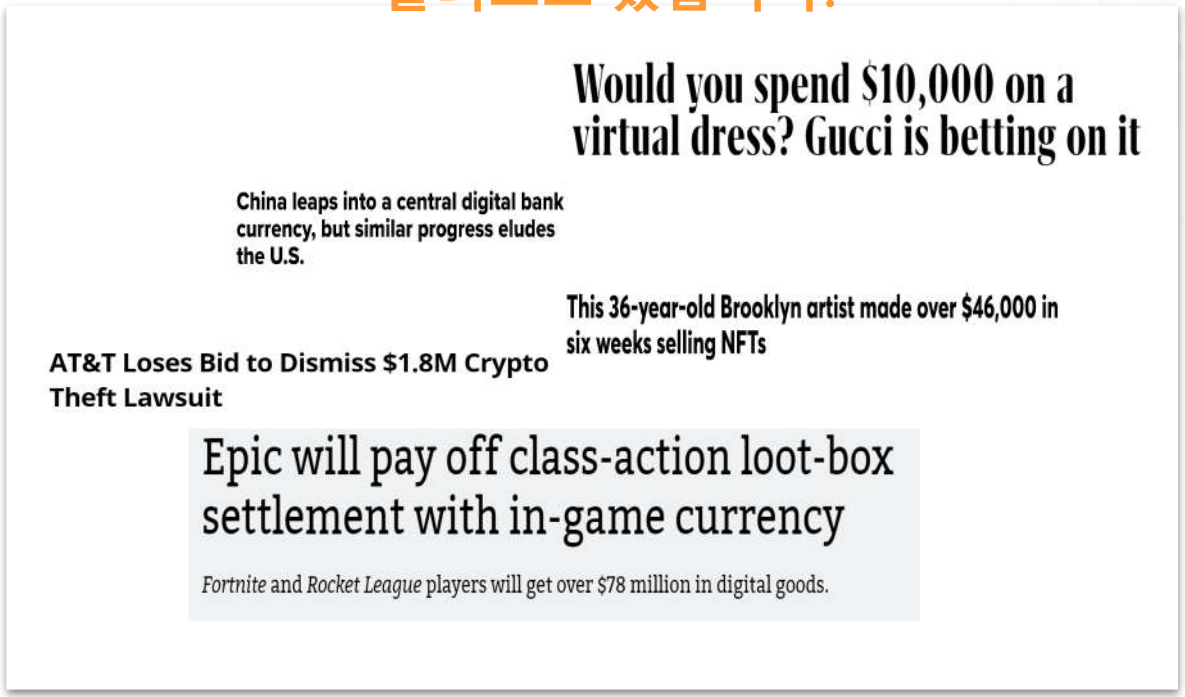
January	59% higher
February	54% higher
March	32% higher

하지만 리스크는 급증하는 반면 신뢰는 추락하고 있습니다.

… 사용자들은 온라인 경험을 신뢰하지 않습니다…



… 그리고 새로운 디지탈 자산은 또다른 위험성을 불러오고 있습니다.



Source: Edelman Trust Barometer 2020

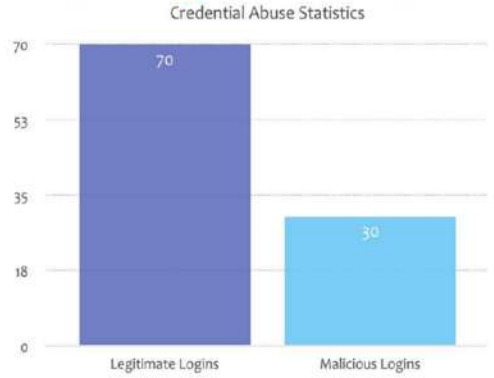
Akamai Experience the Edge

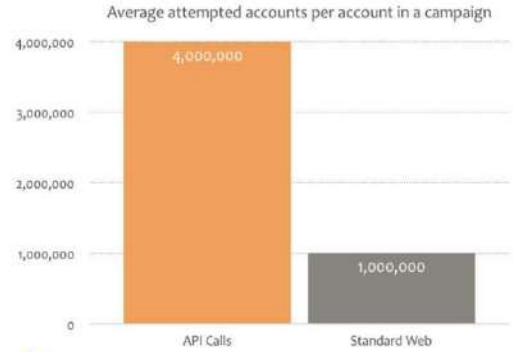
여러분의 디지털 자산은 안전합니까?

Ref: https://www.pexels.com/photo/door-handle-key-keyhole-279810/

재작년 이맘때...

그중 Login에 사용된 비중





API는 기존의 웹 폼과 비교했을 때
성능은 우수하지만 저렴한
비용으로 공격 실행 가능

Akamai Experience the Edge

최근 대규모 피해 사례

'Onliner' malware spambot targets 711 million email accounts

It could be the largest spambot yet.

Data Breach , Data Loss

Breach of 'Verifications.io' Exposes 763 Million Records

Experts Question How 'Big Data Email Verification Platform' Amassed Information

NEWS

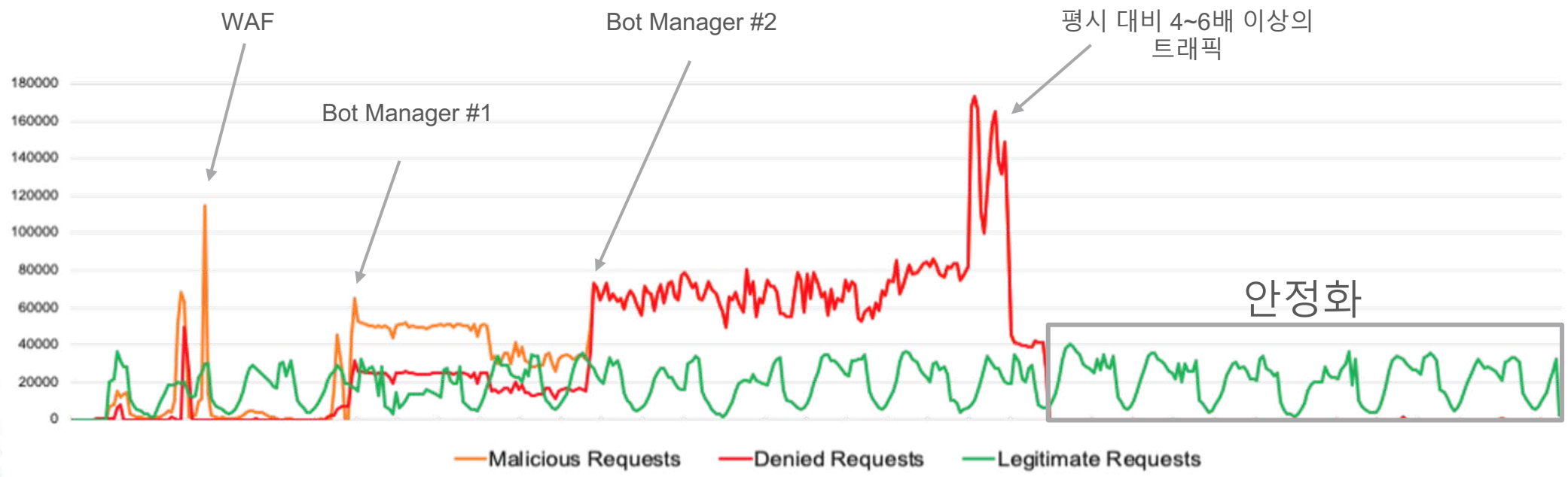
'Collection #1' reveals 773 million email addresses, passwords in one of largest data breaches ever

You can check to see if your username and password have been leaked.

Akamai Experience the Edge

Akamai Experience the Edge

그리고 바로 작년



40,000개의 “clean” IP들이 이 공격에 사용되었습니다.
천백만건의 조합시도가 엣지에서 무력화되었습니다.

계정 탈취, 불법 이용 사이버 킬 체인

크리덴셜 스터핑 (부정 로그인 시행)

계정 탈취 (Account Takeover)

크리덴셜
공급체인

Bot

Human

bot를 사용하여 탈취한 계정으로 로그인을
시도하여 유효한 아이디(ID), 패스워드 쌍 획득

입수한 ID, 패스워드 쌍을「출처」에게
주어 부정구매, 부정송금 등 부정행위 시도

Credential Acquisition

Leverage a botnet to automate validation

Validate credentials against target website

Use compromised account credentials to login

Perform fraudulent actions using compromised

Reconnaissance | Weaponization | Delivery | Exploitation | Action

Akamai

' 봇의 기계적인 행동 ' 을 검증하고
bot에 의한 접근을 억제

개개인의 이용자가 평소 이용하고 있는
환경을 학습하여 다른 사람에 의한
'이상 로그인' 식별

봇 감지

리스크 기반 인증

계정 탈취 체인

Akamai Experience the Edge

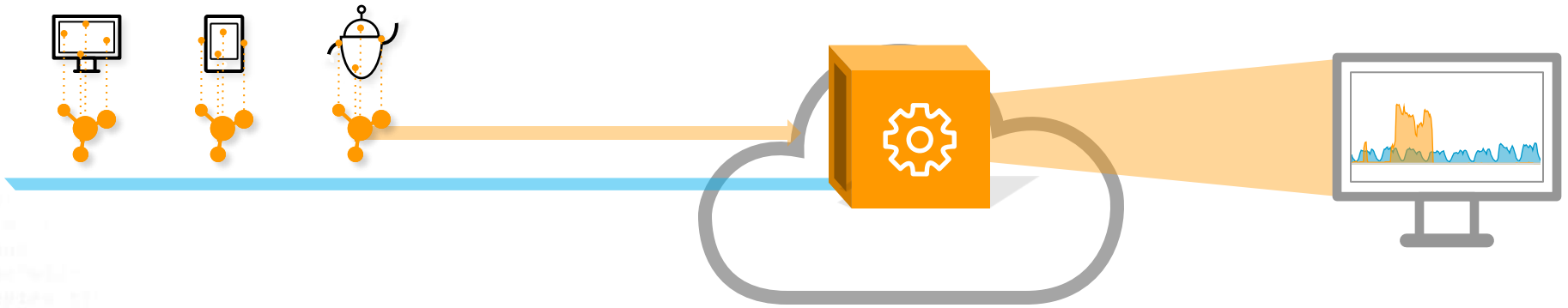
바로 이렇게 말이죠.

공격자의 정교한 우회 기법보다 앞서 나가야 하는 봇 탐지 기술

행동 데이터
클라이언트측 데이터 수집

분석 엔진
비동기식 서버측 분석

봇 탐지
높은 정확도를 갖춘 인간 또는 봇



사용자 행동 시그널

브라우저 + 브라우저 특성

제한된 난독 처리 필요

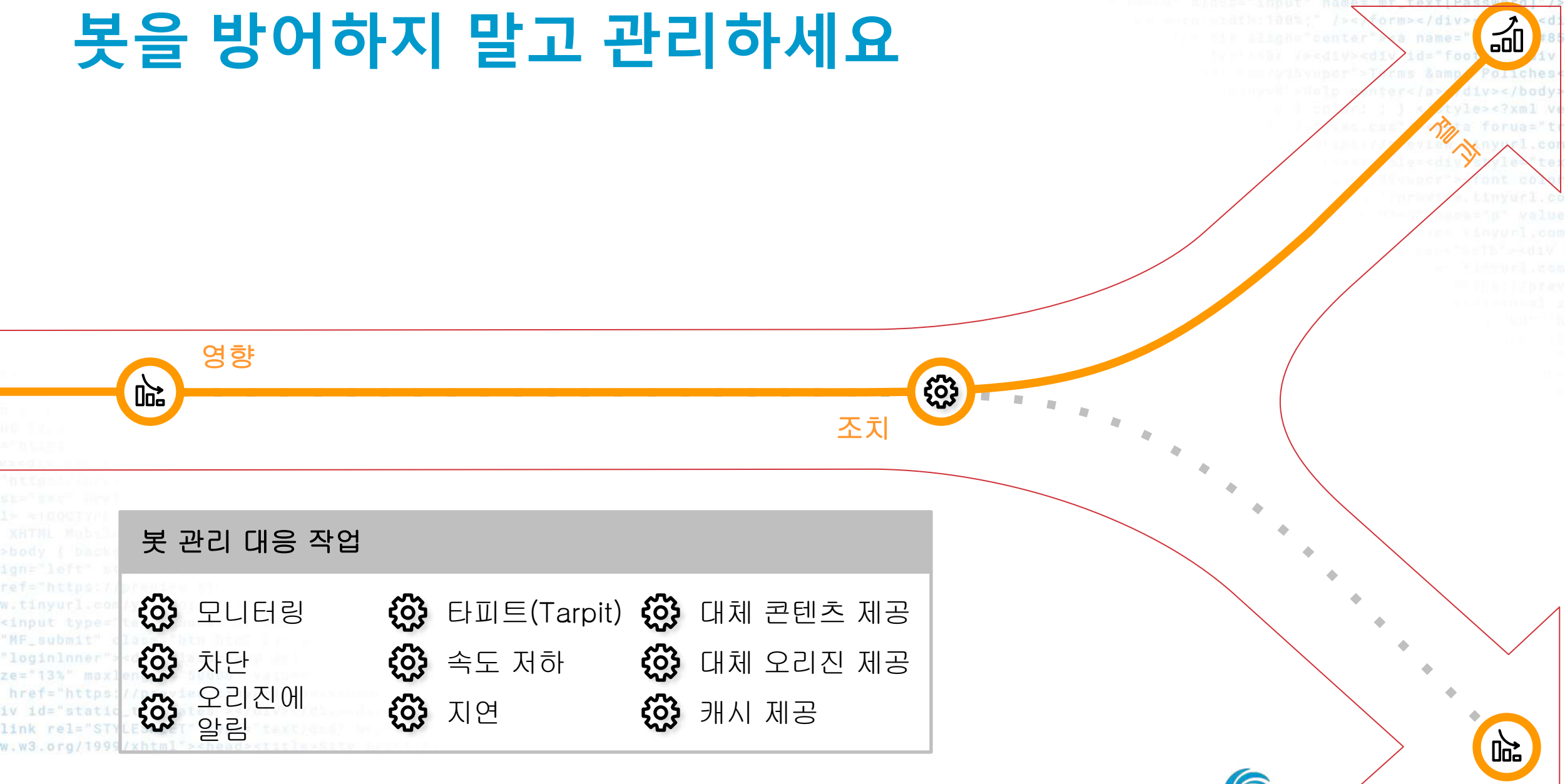
수백 개의 시그널로 처리

위협 인텔리전스로 의사 결정 지원

공격자의 행동 변화에 따라 탐지 기능 조정

Akamai Experience the Edge

봇을 방어하지 말고 관리하세요



봇 관리 대응 작업		
모니터링	타피트(Tarpit)	대체 콘텐츠 제공
차단	속도 저하	대체 오리진 제공
오리진에 알림	지연	캐시 제공

Akamai Experience the Edge

이경우는 어떻게 하죠?

계정 탈취, 불법 이용 사이버 킬 체인

크리덴셜 스터핑 (부정 로그인 시행)

계정 탈취 (Account Takeover)

크리덴셜 공급체인

Bot

Human

bot를 사용하여 탈취한 계정으로 로그인을 시도하여 유효한 아이디(ID), 패스워드 쌍 획득

입수한 ID, 패스워드 쌍을「출처」에게 주어 부정구매, 부정송금 등 부정행위 시도

Credential Acquisition | Leverage a botnet to automate validation | Validate credentials against target website | Use compromised account credentials to login | Perform fraudulent actions using compromised account

Reconnaissance | Weaponization | Delivery | Exploitation | Action

Akamai

' 봇의 기계적인 행동 ' 을 검증하고 bot에 의한 접근을 억제

개개인의 이용자가 평소 이용하고 있는 환경을 학습하여 다른 사람에 의한 '이상 로그인' 식별

봇 감지

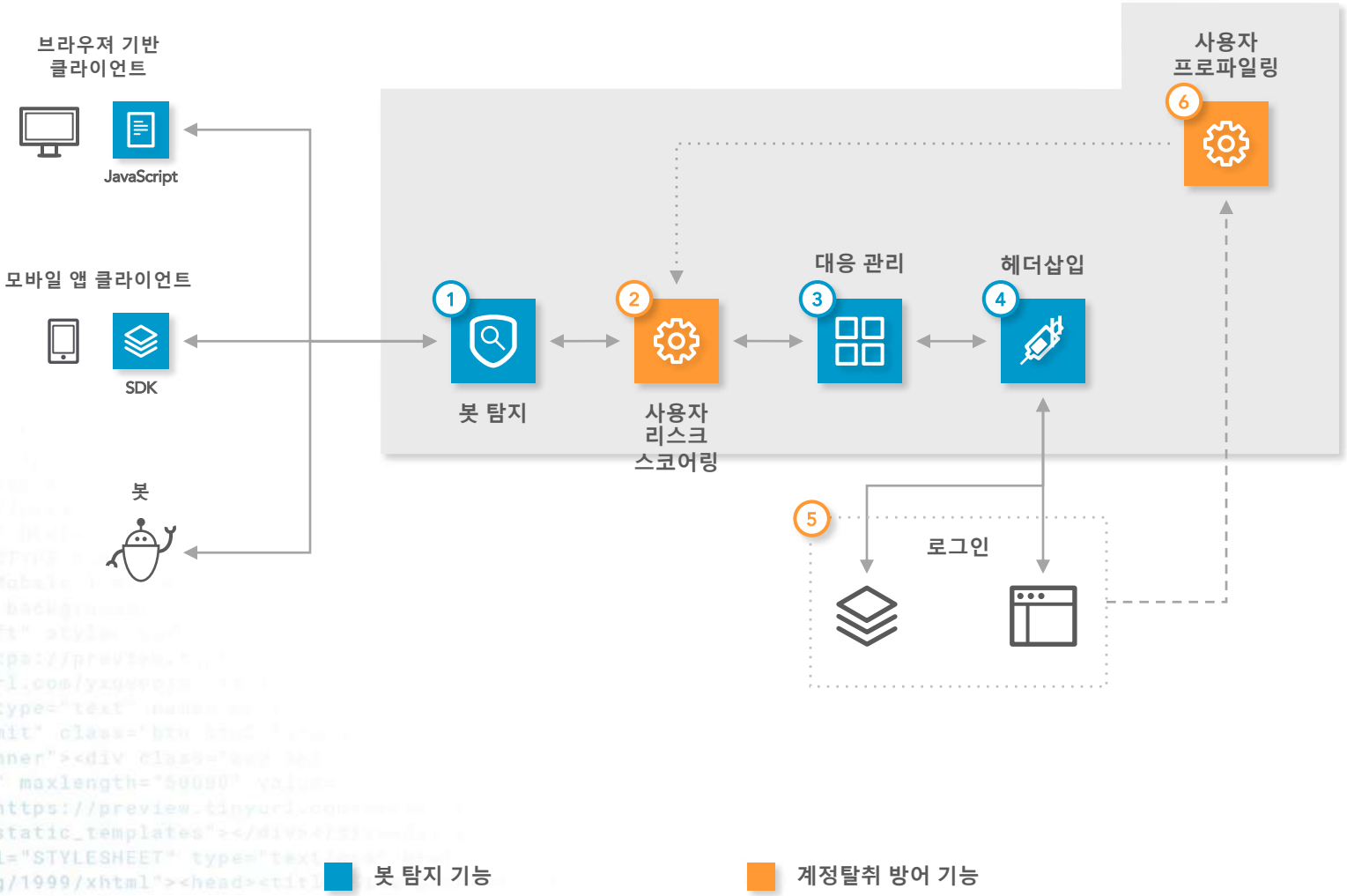
리스크 기반 인증

계정 탈취 체인

Akamai Experience the Edge

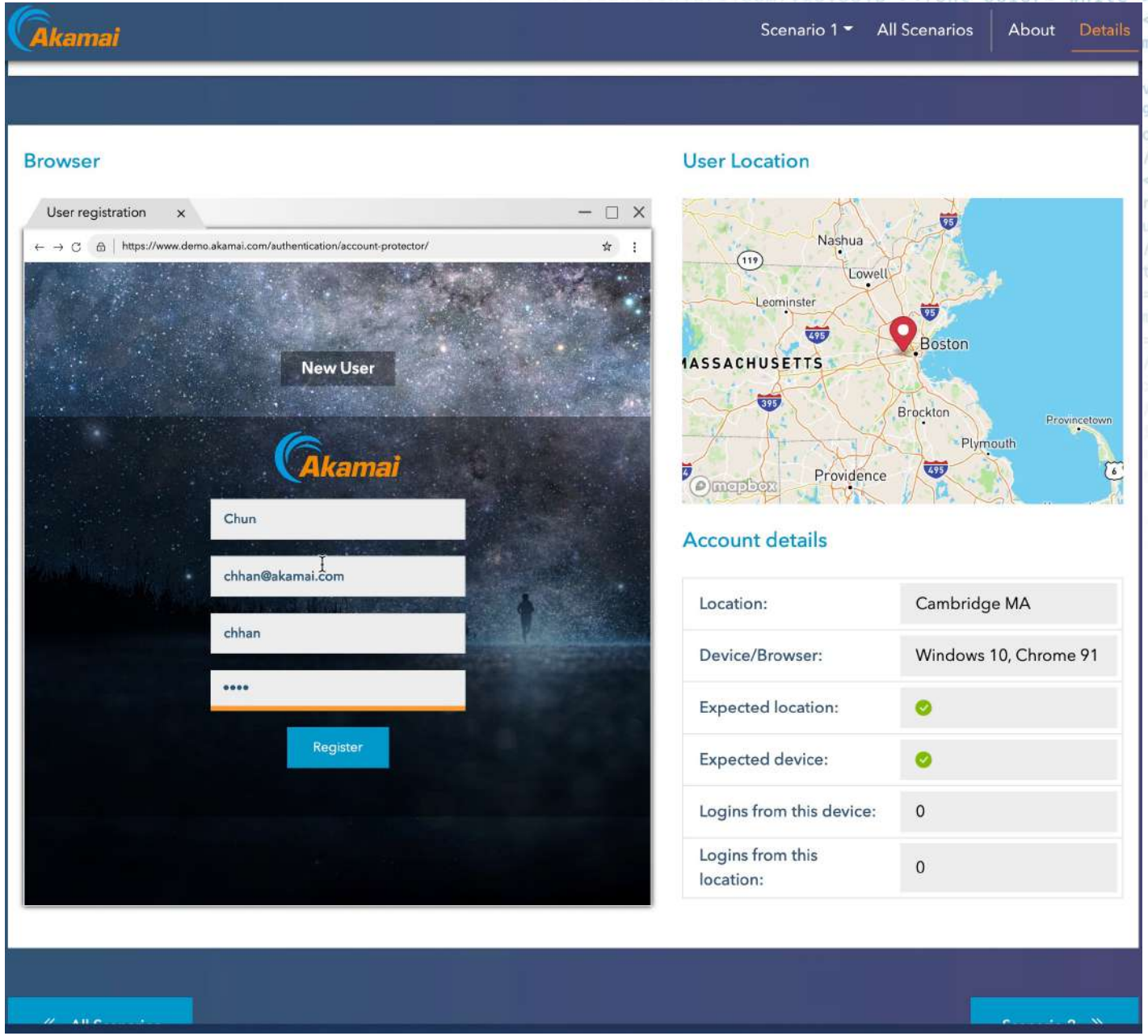
계정탈취 방어를 위한 아키텍쳐

Reference Architecture



1. 머신러닝 알고리즘 및 수백가지의 시그널을 활용하여 정교한 봇들에 대한 엣지단에서의 탐지 진행 및 대응.
2. 머신러닝 데이터를 활용한 사용자의 신뢰성을 엣지단에서 검증.
3. 고객은 차단, 대체서비스 또는 오리진으로의 전송을 포함하여 봇이나 계정탈취범이 보낸 요청에 대해 서로다른 관리작업을 구성할 수 있음.
4. 엣지에서 사용자의 요청에 식별인자를 헤더에 주입하여 원본에 전달.
5. 고객은 단계적 인증 또는 추가 부정행위의 상관관계확인등의 추가 조치가 가능
6. 사용자 프로파일링은 로그인시 확인되는 여러 위험요소를 기반으로 향후 로그인 시도를 평가하고 스코어링

예시: New User

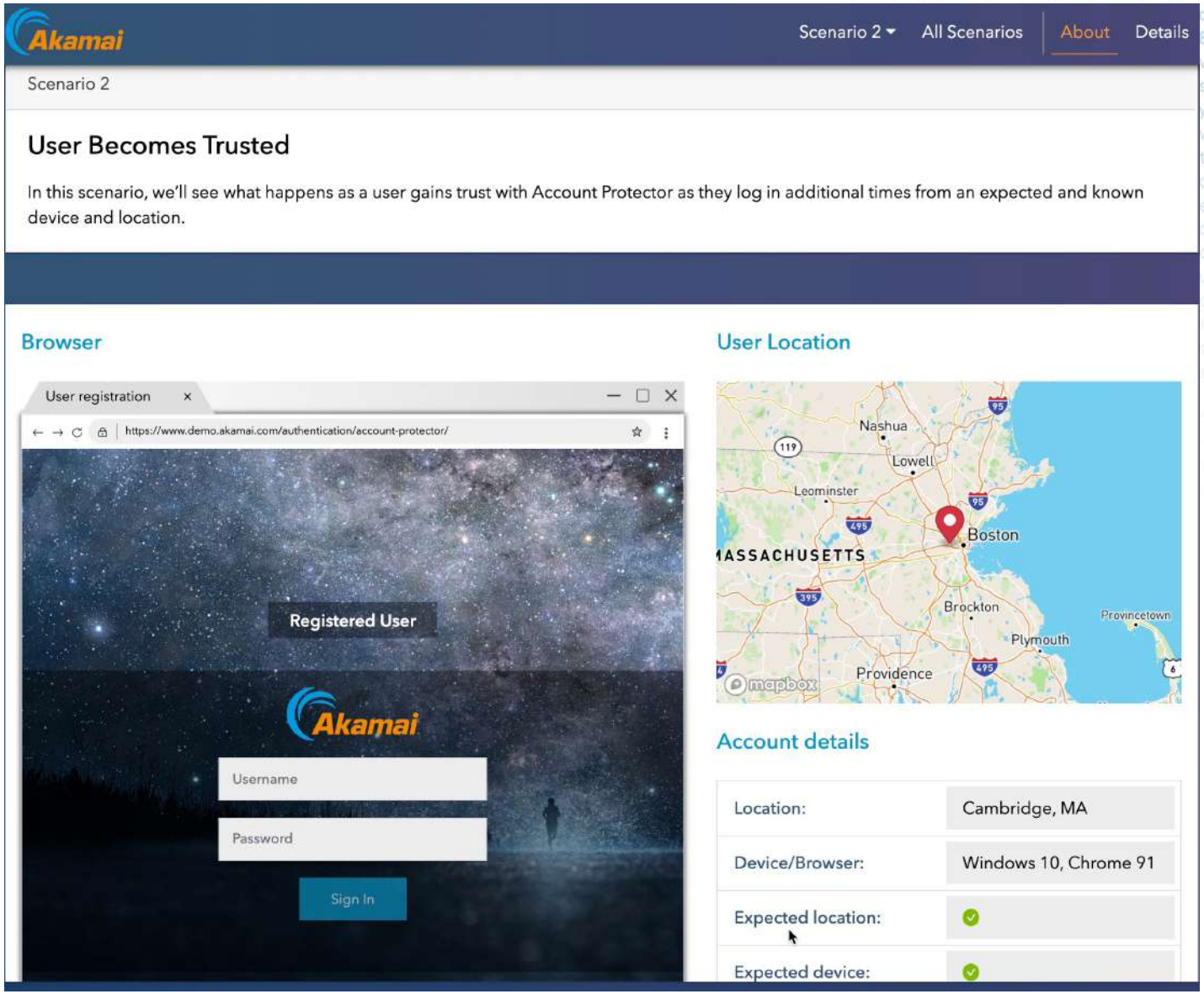


```
Akamai-User-Risk: uuid=964d54b7-0821-413a-a4d6-
8131770ec8d5;requestid=59855ee1;status=2;score=30;risk=udfp:de08d356f46d1f1062e1f1f219121ab8e82696a4/L|ugp:
us/L|unp=20057/L;general=di=d1f75f3a3224d413e5e1de5c3bf7578d337023f3|do=Windows 10|db=Chrome
91|aci=0;allow=0;action=none
```

Field ID	Description	
uuid	아카마이에서 생성한 임의의 UUID	964d54b7-0821-413a-a4d6-8131770ec8d5
requestid	분석을 위한 엣지로의 요청 ID	59855ee1
status	우측표	2
score	사용자 리스크 스코어로 0~100사이며, 높을수록 위험이 크다는 의미입니다.	30
general	요청에 대한 일반적인 정보	di=d1f75f3a3224d413e5e1de5c3bf7578d337023f3|do=Windows 10|db=Chrome 91|aci=0
risk	리스크를 높인 위험지표	udfp:de08d356f46d1f1062e1f1f219121ab8e82696a4/L|ugp:us/L|unp=20057/L
trust	신뢰지표	
allow	사용자가 허용 리스트에 추가여부의 플래그 지표	0
action	계정탈취 보호 액션대응 여부 지표	none

Scoring Status	Description
0	정상
1	오류
2	사용자 프로파일 없음
3	사용자 프로파일 부족으로 정확한 점수불가
4	이 클라이언트에서 수신된 텔레메트리 없음
5	계산시간 초과
6	로그인 폼에서 사용자 이름 없음
7	비 로그인 요청서 사용자 프로파일과 BMP쿠키 매칭 안됨

예시: Trusted User

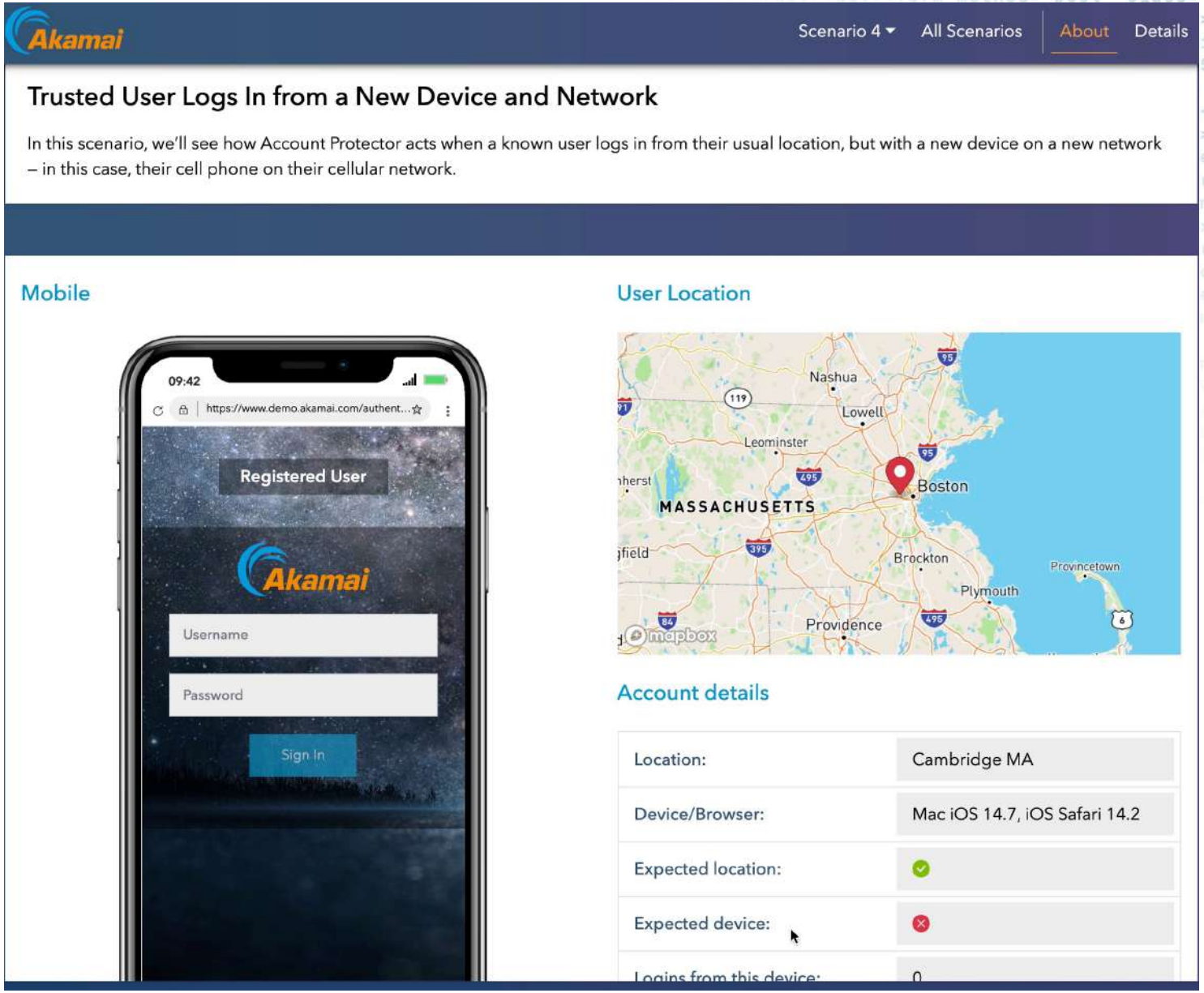


```
Akamai-User-Risk: uuid=964d54b7-0821-413a-a4d6-
8131770ec8d5;requestid=1b6c092c;status=3;score=17;risk=udfp:de08d356f46d1f1062e1f1f219121ab8e82696a4/L|ugp:
us/L|unp=20057/L;general=di=d1f75f3a3224d413e5e1de5c3bf7578d337023f3|do=Windows 10|db=Chrome
91|aci=0;allow=0;action=none
```

Field ID	Description	
uuid	아카마이에서 생성한 임의의 UUID	964d54b7-0821-413a-a4d6-8131770ec8d5
requestid	분석을 위한 엣지로의 요청 ID	1b6c092c
status	우측표	3
score	사용자 리스크 스코어로 0~100사이며, 높을수록 위험이 크다는 의미입니다.	17
general	요청에 대한 일반적인 정보	di=d1f75f3a3224d413e5e1de5c3bf7578d337023f3|do=Windows 10|db=Chrome 91|aci=0
risk	리스크를 높인 위험지표	udfp:de08d356f46d1f1062e1f1f219121ab8e82696a4/L|ugp:us/L|unp=20057/L
trust	신뢰지표	
allow	사용자가 허용 리스트에 추가여부의 플래그 지표	0
action	계정탈취 보호 액션대응 여부 지표	none

Scoring Status	Description
0	정상
1	오류
2	사용자 프로파일 없음
3	사용자 프로파일 부족으로 정확한 점수불가
4	이 클라이언트에서 수신된 텔레메트리 없음
5	계산시간 초과
6	로그인 폼에서 사용자 이름 없음
7	비 로그인 요청서 사용자 프로파일과 BMP쿠키 매칭 안됨

예시: Trusted User from new device and network



```
Akamai-User-Risk: uuid=964d54b7-0821-413a-a4d6-
8131770ec8d5;requestid=23bb86d1;status=0;score=61;risk=udfp:63aa8af33817e167ba8a043ea4470e669315f004/H|unp=
20057/H;trust=ugp:us;general=di=40cb14d05d0166bd7f2a4c7ec603d05b7a632f3f|do=Mac iOS 14|db=iOS Safari
14|aci=0;allow=0;action=none
```

Field ID	Description	
uuid	아카마이에서 생성한 임의의 UUID	964d54b7-0821-413a-a4d6-8131770ec8d5
requestid	분석을 위한 엣지로의 요청 ID	23bb86d1
status	우측표	0
score	사용자 리스크 스코어로 0~100사이며, 높을수록 위험이 크다는 의미입니다.	61
general	요청에 대한 일반적인 정보	di=40cb14d05d0166bd7f2a4c7ec603d05b7a632f3f|do=Mac iOS 14|db=iOS Safari 14|aci=0
risk	리스크를 높인 위험지표	udfp:63aa8af33817e167ba8a043ea4470e669315f004/H|unp=20057/H
trust	신뢰지표	ugp:us
allow	사용자가 허용 리스트에 추가여부의 플래그 지표	0
action	계정탈취 보호 액션대응 여부 지표	none

Scoring Status	Description
0	정상
1	오류
2	사용자 프로파일 없음
3	사용자 프로파일 부족으로 정확한 점수불가
4	이 클라이언트에서 수신된 텔레메트리 없음
5	계산시간 초과
6	로그인 폼에서 사용자 이름 없음
7	비 로그인 요청서 사용자 프로파일과 BMP쿠키 매칭 안됨

악의적 사용자 활동에 대한 조사

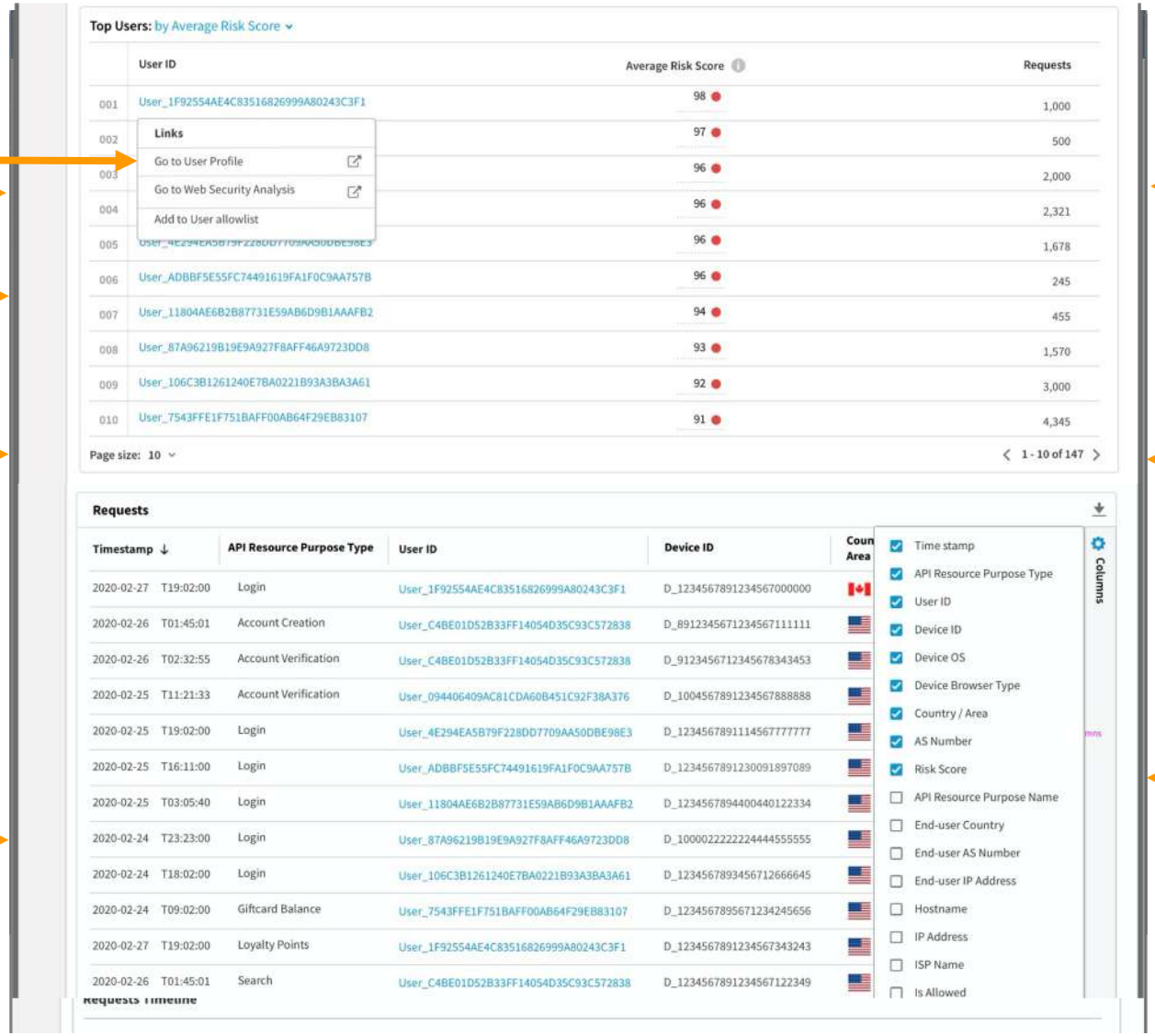
특정 사용자를 조사하기 위해 사용자 프로파일로 이동합니다.

사용자의 UUID또는 username으로 검색합니다.

보호하는 엔드포인트에서 사용자 활동 요약을 검토합니다.

평균 위험 레벨별 사용자 분석을 검토합니다.

최근 요청 – 추가 요청 정보를 보기위해 필드를 선택합니다.



심층 조사를 위해 사용자 활동을 필터링 합니다.

다양한 용도별 API를 유형별로 사용자의 활동 및 위험 레벨을 파악할 수 있습니다.

부정 사용자의 활동을 식별하고 조사하기위해 위험 레벨과 행동 타임라인을 요청합니다.

Akamai Experience the Edge

Akamai is Recognized by Top Analysts

FORRESTER®

Leader, The Forrester Wave™

봇 관리 부문,
Q1 2020

 |

Akamai Experience the Edge

계정 탈취 방어, 이젠 선택이 아닌 필수입니다.

Akamai Experience the Edge