금융 기업을 위한 Intelligence 기반의 보안전략

EMC RSA Division

2014.11

EMC²

Agenda

- 보안 트랜드
- Fraud & Risk Intelligence
- RSA 대응 전략
  - 웹 행위 모니터링
  - 위험 분석 기반 인증
  - 피싱/계정 유출 탐지
- 기대효과

보안 트랜드

BILLIONS
OF USERS

3RD PLATFORM
2010

Mobile Cloud Big Data Social

Mobile Devices

MILLIONS
OF APPS

HUNDREDS OF MILLIONS
OF USERS

2ND PLATFORM
1990

LAN/Internet Client/Server

PC

TENS OF THOUSANDS
OF APPS

MILLIONS
OF USERS

1ST PLATFORM
1970

Mainframe, Mini Computer

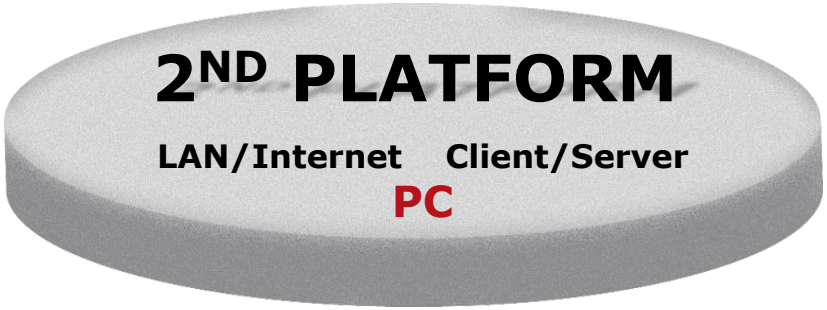
Terminals

THOUSANDS
OF APPS

Source: IDC, 2012

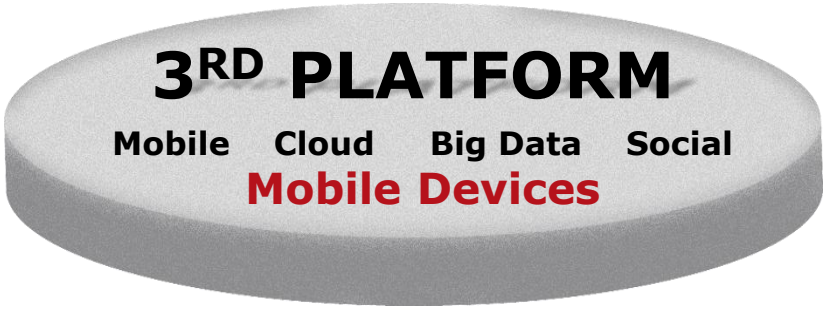
EMC²

보안에 대한 새로운 접근 요구



IT 통제
경계 보안

예방
SIGNATURE-BASED



사용자 중심
탈 경계 보안

탐지
INTELLIGENCE-DRIVEN

EMC²

Intelligence-Driven Security

VISIBILITY

사건에 대한 데이터 수집
위험 – 네트워크 트래픽 – Identity - 트랜젝션

ANALYSIS

보안 위협이 있는 이상행위 탐지

ACTION

비즈니스 손실을 최소화 할 수 있는 조치

EMC²

RSA's Focus Areas

Fraud & Risk Intelligence

웹 사기 행위 사례

구분	A사 모바일 상품권	B사 홈페이지	C사 앱카드
사건 요약	A사 타인 명의의 모바일 상품권 구입	**B사 홈페이지에서 대규모 회원정보 불법취득**	타인 명의의 C사 앱카드 발급
사건 경위	해커가 A사 몰 가입자 정보를 스미싱을 통해 수집 후 탈취한 계정정보를 통해 사이트를 접속하여 모바일 상품권을 구입한 것으로 추정	해커가 B사의 이용대금명세서 고유번호 9자리를 무작위로 웹페이지에 입력해 회원정보 취득	스미싱을 통해 C사 회원의 주민번호와 전화번호 등 탈취 후 타인명의의 앱카드를 신청하여 결재
사건유형	계정 도용	계정 탈취 패스워드 추측 공격 비즈니스 로직 악용 (명세서의 고유번호를 통해 로그인 회원 이외의 정보도 확인할 수 있는 로직 취약점)	계정 도용 비즈니스 로직 악용 (아이폰 본인 확인 로직 취약점)
피해 규모	49명, 248만 5,000원	1,200만명 회원정보 취득	53명, 300건 6,000만원

웹 사기 행위 시사점

- 스미싱과 같은 사회공학적 방법으로 악성 사이트 접근 유도
- 다양한 경로로 탈취한 계정정보를 도용한 사기행위
- 비즈니스 로직의 헛점을 이용한 정보 불법 취득
- 스크립트에 의한 자동화된 시스템 접근
- 고객정보 유출이 실제 금전적인 피해로 확산됨

EMC²

이상행위 대응방안

이상행위 대응방안

웹 행위 모니터링
(계정도용, 비즈니스 로직 악용, 사이트 스크랩핑)

위험분석 기반
차별화된 인증 요청

위험분석 기반
카드 인증 요청

피싱/유출계정
탐지/차단

부정 거래내역
모니터링

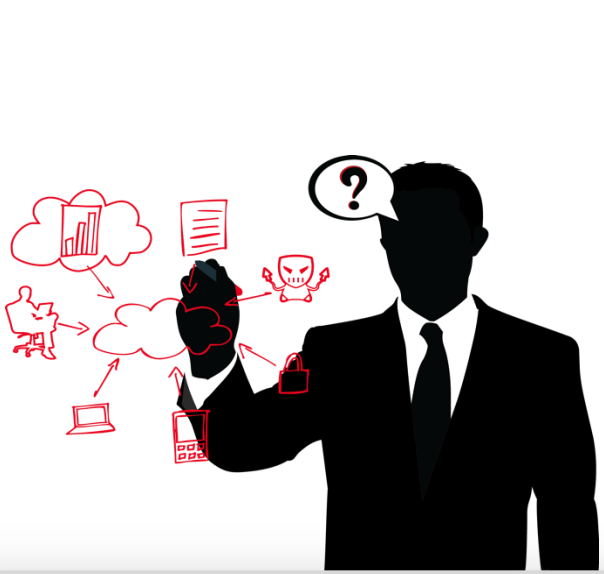
오픈웹 | 세션시작 | 로그인 | 거래 | 로그아웃

웹 위협 환경

RSA 대응 전략

RSA 이상행위 대응 솔루션

전체 온라인 사기 행위 보호방안



RSA Web Threat Detection

RSA Adaptive Authentication

RSA Adaptive Authentication for eCommerce

RSA Transaction Monitoring

Fraud Action

오픈웹 세션시작 로그인 거래 로그아웃

웹 위협 환경

RSA 이상행위 대응 솔루션 비교

	RSA WTD	RSA AA	RSA FAS
알려진 사기행위 탐지	●	●	N/A
새로운 사기행위 분석 탐지	●	○	N/A
인증 및 거래 행위 상세 모니터링	●	●	N/A
자기 학습 기능 제공	●	●	N/A
실시간 사기 행위 대응(경보 또는 차단)	●	○(일부 적용 페이지)	N/A
MITM 및 MITB 탐지	●	●	N/A
비즈니스 우회 공격 탐지	●(모든 페이지)	○(일부 페이지)	N/A
거래 차단 또는 확인	○(F5 연동)	●(세션 차단/재인증)	N/A
웹서버 기능 변경	없음	스크립트 삽입필요	없음
유출된 고객 정보 확인	N/A	N/A	●
피싱/파밍 사이트 탐지 및 차단	N/A	N/A	●

EMC²

RSA 웹 행위 모니터링

- RSA Web Threat Detect

RSA Web Threat Detection

웹 세션 정보 분석 소프트웨어

- 웹사이트 위협 탐지, 사기 및 기타 공격 방지
- Self Learning을 통한 위협 분석
- 실시간 위협에 대한 가시성 제공
- 사용자와 서비스에 영향을 주지 않는 구성 지원

정상적인 사용자와 비정상적인 사용자 구별

전체 웹세션에 대한 가시성 확보 필요

빅데이터 분석 및 가시성 활용

전체 웹 세션에 대한 가시성을 통한 계속적인 모니터링 필요

전체 사용자와 개별 사용자를 분석 할 수 있는 능동적 행위 분석 프로파일 필요

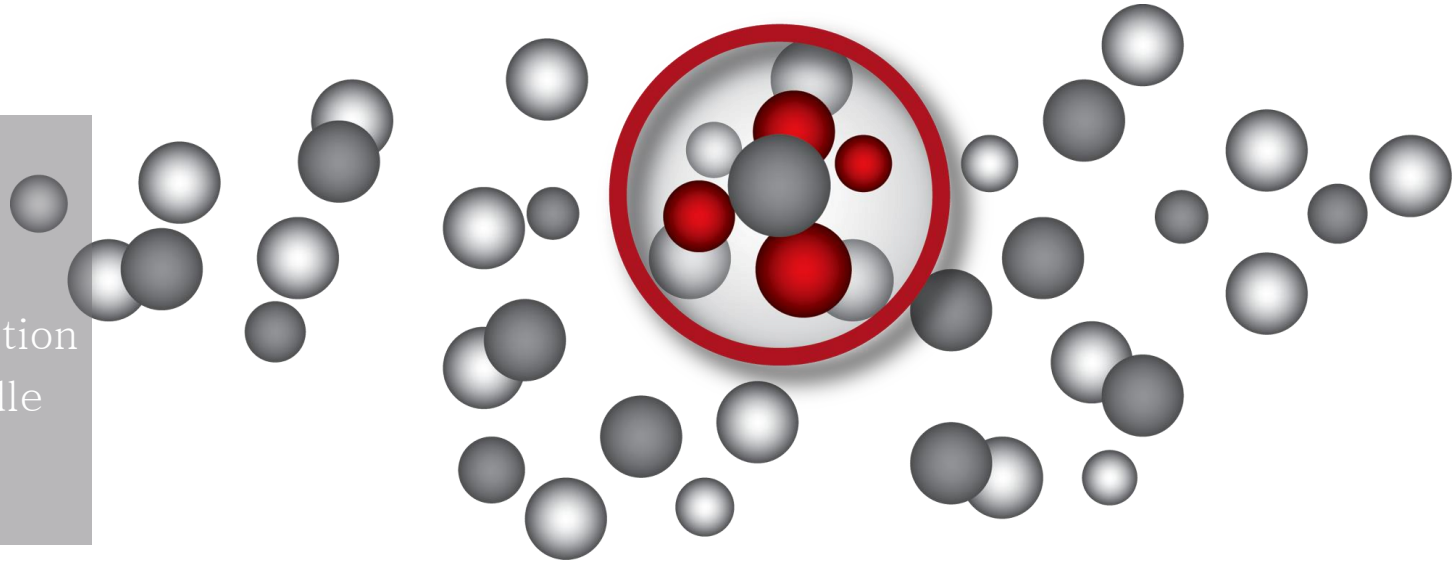
정책 생성을 통한 스코어링 기반 실시간 위협 분석

EMC²

스트림 분석

위협 스코어링

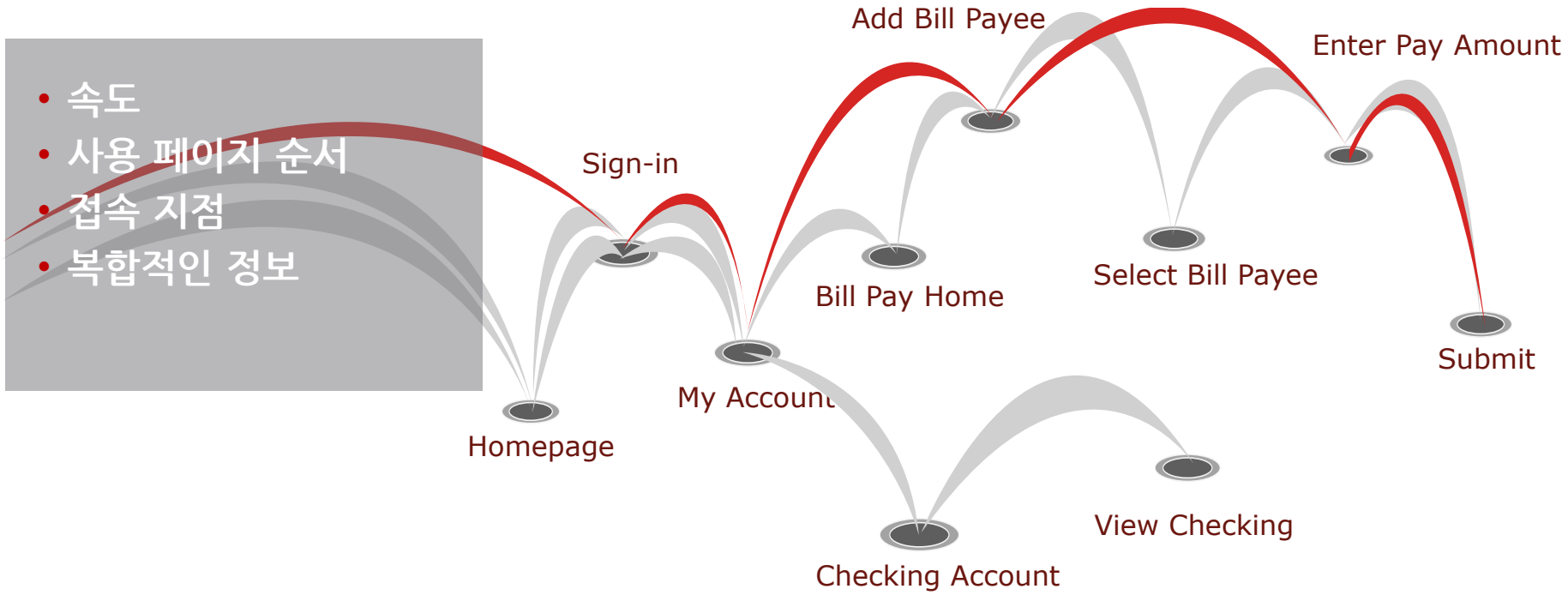
- 속도
- 웹 사용 행위
- Parameter Injection
- Man in the Middle
- Man in the Browser



이상 행위 탐지

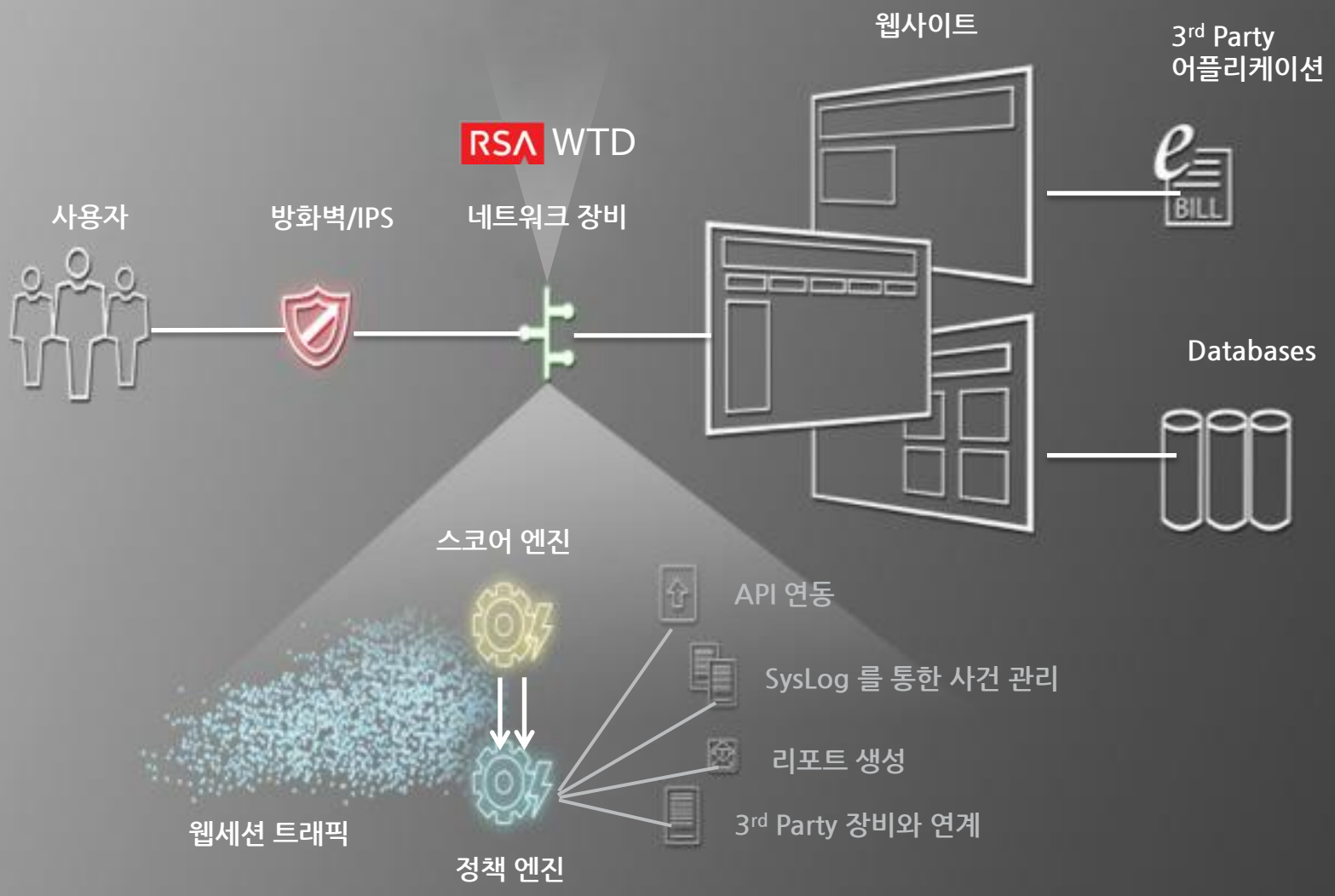
사이버 범죄행위 자들은 일반적인 온라인 사용자와 다른 사용 패턴을 보임

- 속도
- 사용 페이지 순서
- 접속 지점
- 복합적인 정보



RSA Web Threat Detection

웹세션 정보 분석을 통한 웹 사이트 방어



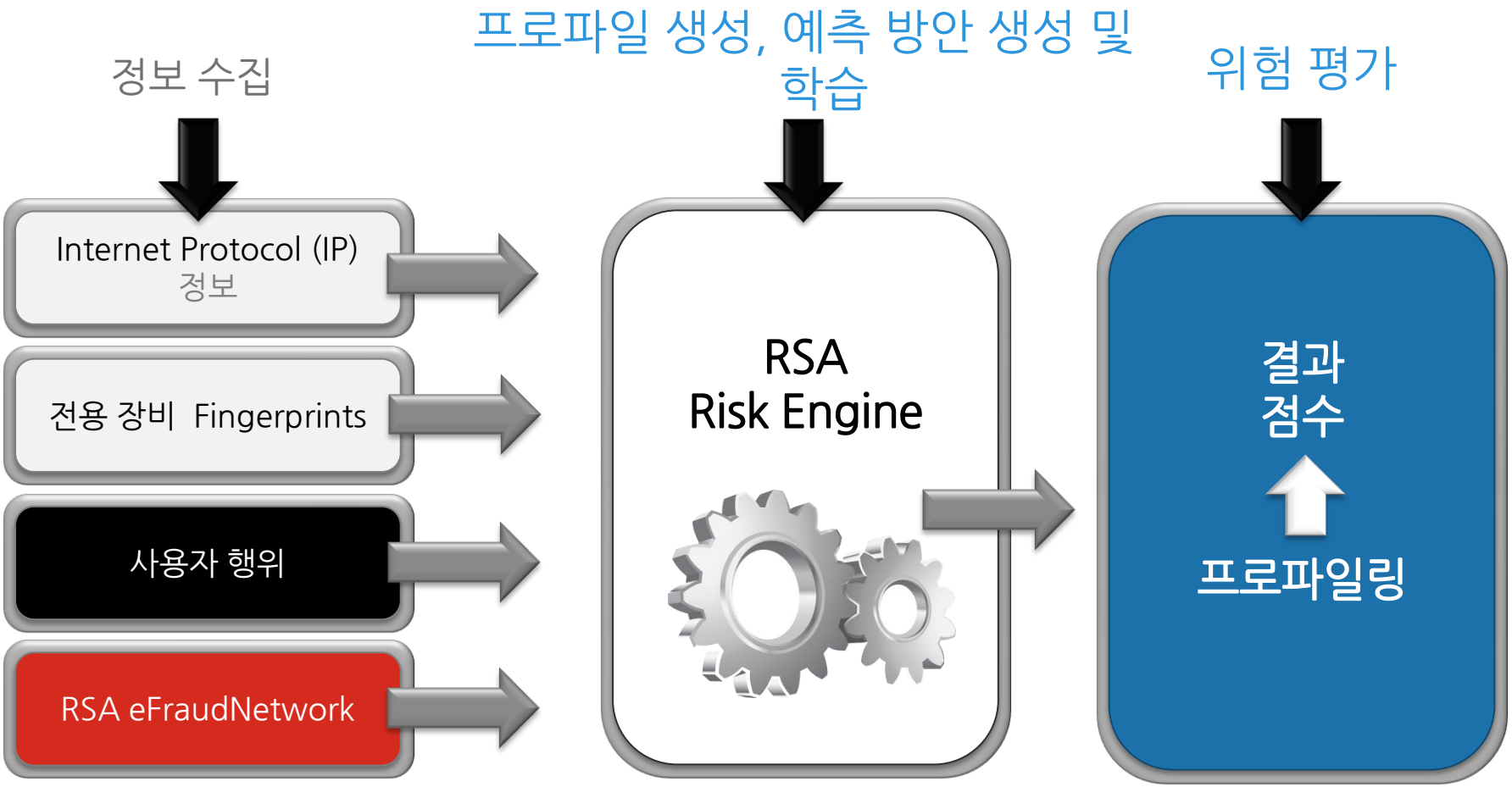
RSA 위험 분석 기반 인증

- RSA Adaptive Authentication

RSA 위험 기반 인증 솔루션

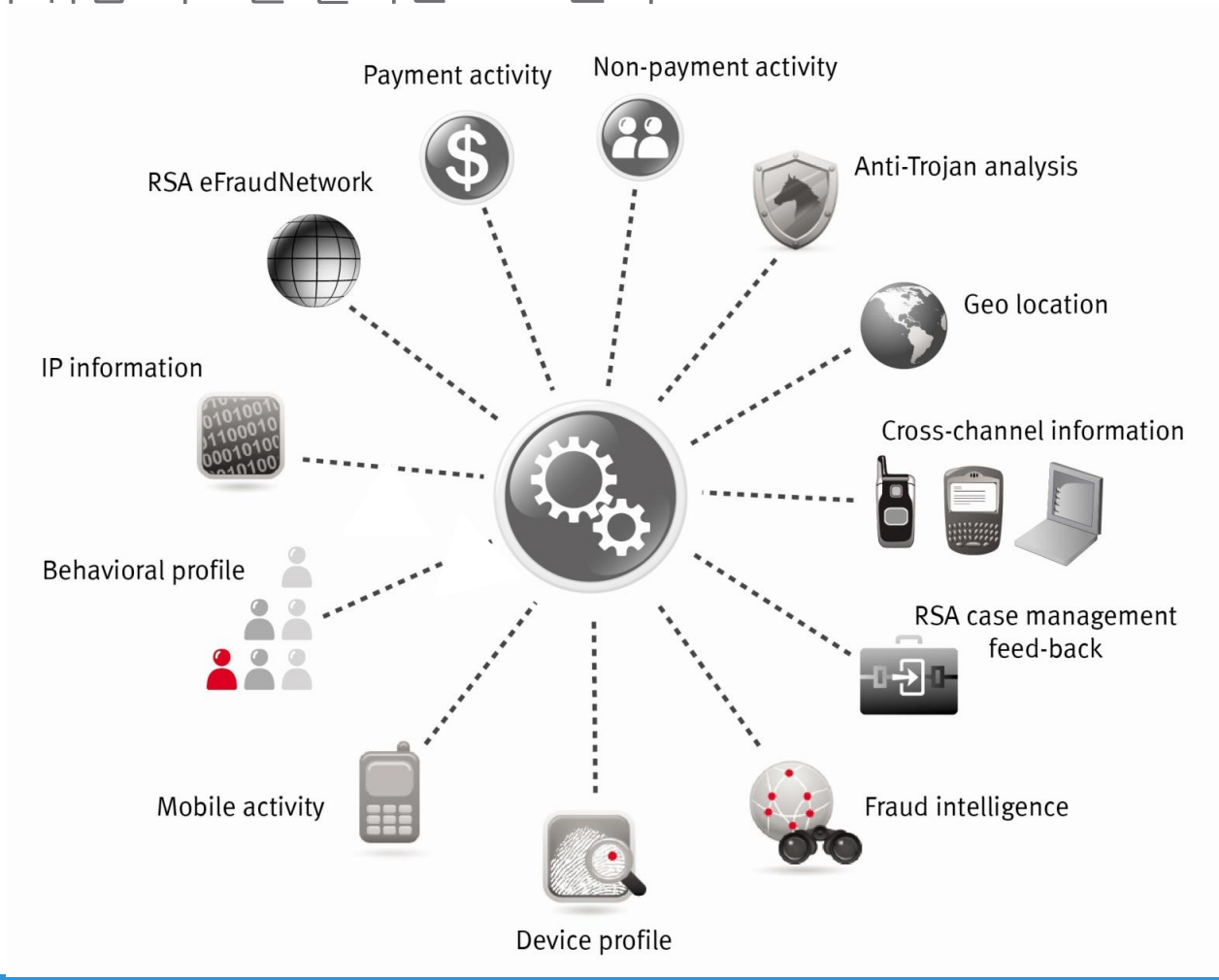
- 포괄적인 인증 체계와 사기 탐지 플랫폼
- 위험 기반(Risk-Based) 인증 기술을 통한 인증 강화
  - 사용자 로그인 시, 로그인 이후의 행위를 통한 위험 산출
  - 위험, 정책, 사용자 군에 기반하여 필요한 인증 수준을 설정

RSA 위험 기반 엔진 동작 방식



RSA 위험 기반 엔진

100개 이상의 위험 척도를 실시간으로 분석



RSA 온라인 사기 대응 커뮤니티

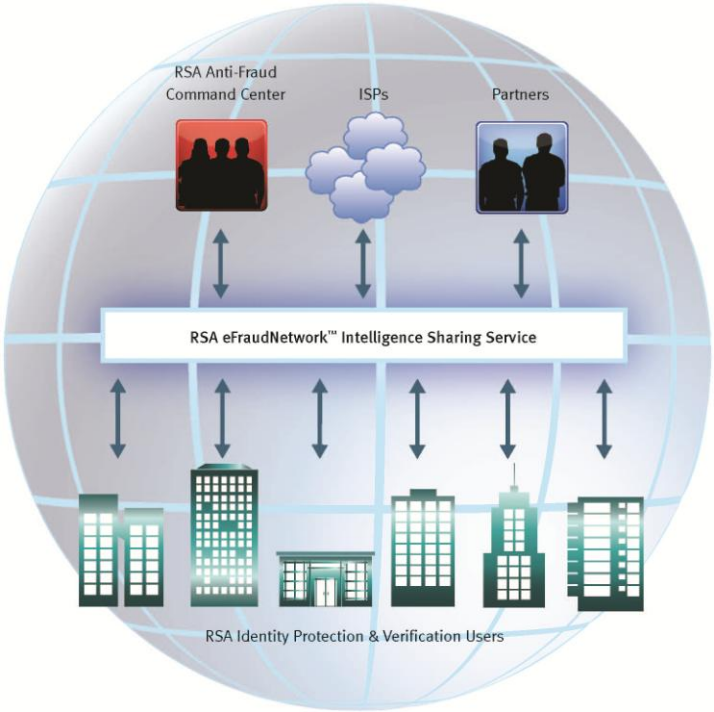
RSA eFraud Network

광범위한 협력체계
고객, 파트너, ISP 및 RSA 조사 분석팀으로 구성

활용도 높은 정보
Intelligent 점수 및 피드백, 정제된 데이터를 통해 산출된 정보

중요 데이터 공유 없음
개인정보 및 정보 취득시 획득된 중요 데이터에 대한 공유 없이 오직 사기 행위 패턴만을 공유

사기 행위 공동 대응
단순 데이터 공유가 아닌 커뮤니티를 통한 사기 행위 공동 대응 체계



RSA 인증 및 대응 방법

사용자 인증을 위한 추가 요소 또는 절차(기본 제공)

Challenge 질의

- 선택된 비밀 질문을 하고 사용자가 등록한 응답 전송

부가 인증

- 임시 인증 번호를 전화로 알려주거나 SMS, Email 등으로 전송
- 거래 금액과 같은 거래 상세 내역 포함 전송

동적 Knowledge-Based Authentication (KBA)

- 실시간으로 사용자에 특화된 동적 질의 생성
- RSA Identity Verification service (US,UK 가능)

멀티 인증 프레임

- "in-house" 개발 또는 3rd Party 방안 사용 허용 -RSA Professional Services 계약 필요

RSA 피싱/계정 유출 탐지

- RSA Fraud Action

RSA FraudAction

Anti-Fraud Command Center (AFCC)

최대 규모의 Phishing, Pharming, Trojan 탐지 및 차단 조직

- 다년간의 군 정보부 경력 가진
  150명 이상의 온라인 사기 분석 인력
- 1주일에 약 15만개의 악성코드 분석
- 사기행위 모니터링 및 사전징후 조사
- Email, Domain, Weblog 모니터링
- 24/7 무중단 운영

Blocking Partner

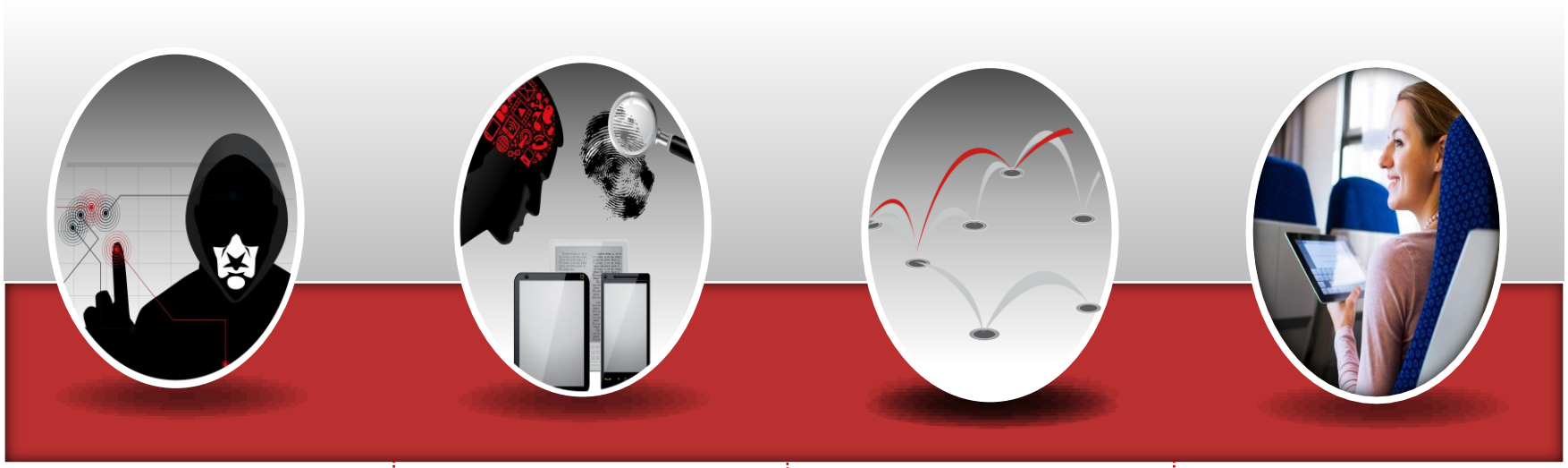
Google Microsoft YAHOO! MS IE & MSN Toolbar Phishing Website

EMC²

기대효과

웹 사기 행위 대응 기대 효과

비정상/악의적인 행위 분석 및 인증 강화를 통한
비즈니스 손실 최소화 및 서비스 신뢰도 강화



악성코드에 의한 고객 정보 유출 내역 확인을 통한 사기행위 사전 대응

위험 기반 인증 강화를 통한 로그인시, 거래시 위험 대응 강화

웹에서 발생하는 모든 행위 분석을 통한 신규 위험 감지

고객에게 보안 강화 및 편의 제공

EMC²

EMC²®