클라우드 웹 방화벽의 정석

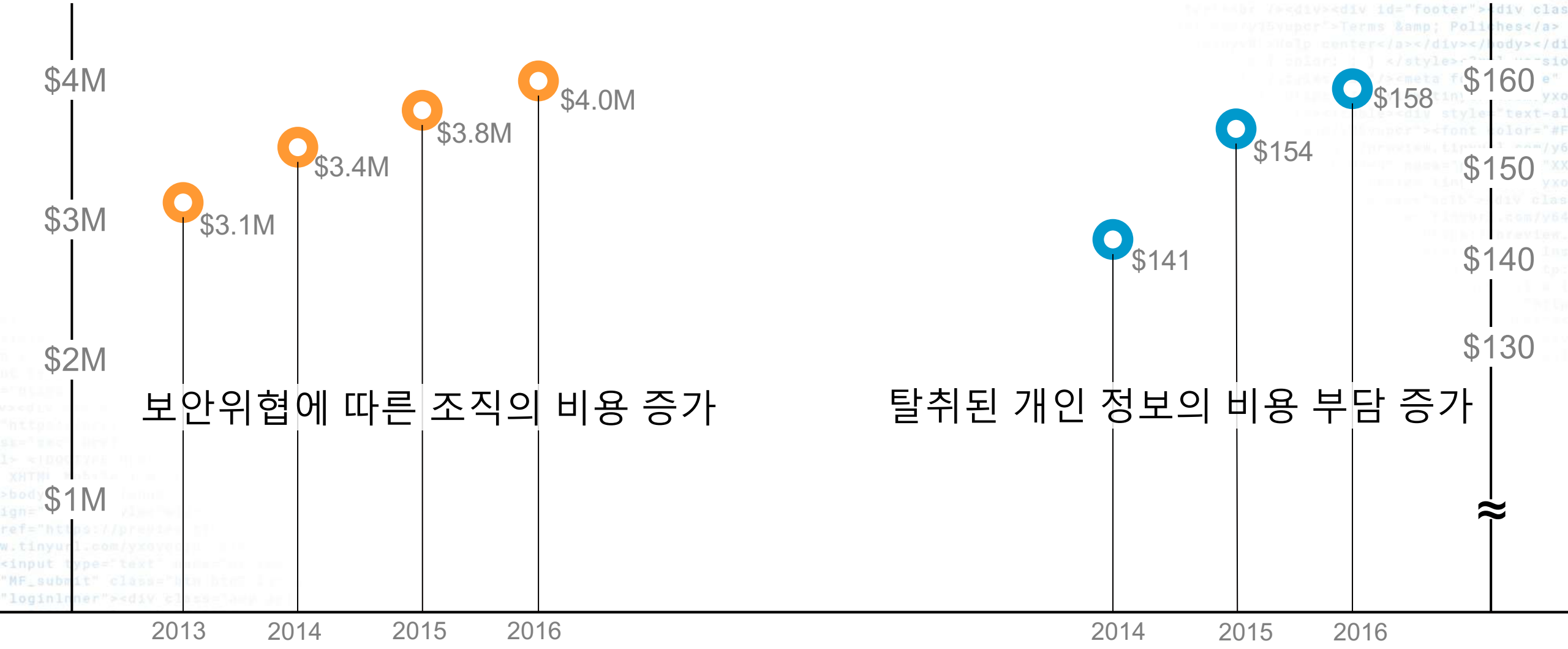
KSD와 적응형 보안 엔진

발표 순서

- 보안 위협 트렌드 분석
- 웹 어플리케이션 아키텍쳐와 공격 예상 지점
- 클라우드 웹 방화벽을 이용한 보안 아키텍쳐
- Kona Site Defender
- 관리형 보안 서비스
- 요약

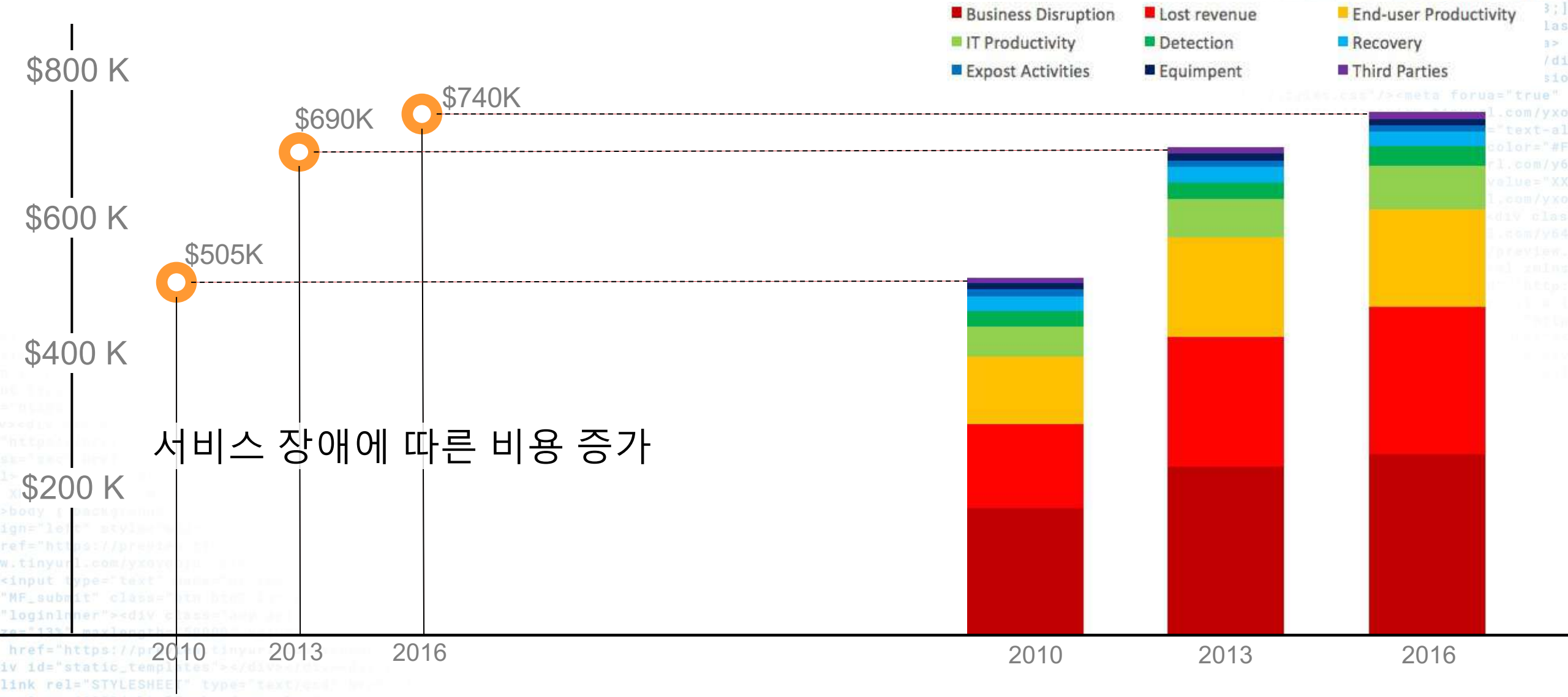
보안 위협 트렌드 분석

숫자로 보는 보안 위협 증가



Source: Ponemon Institute 2016. Part of IBM

숫자로 보는 보안 위협 증가



서비스 장애에 따른 비용 증가

보안 담당자의 업무 중

- 조직의 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위협을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.

출처 : 정보보호 및 개인정보보호 관리체계 인증 - 1.2 위험관리

보안 담당자의 업무 중

- 조직의 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 **연 1회 이상** 위협을 평가하며, **수용할 수 있는 위험**은 경영진의 승인을 받아 관리하여야 한다.

출처 : 정보보호 및 개인정보보호 관리체계 인증 - 1.2 위험관리

위험 수준 판단

- 모든 위험에 대응하거나 위험을 완전히 제거하는 것은 불가능
- 100원짜리 정보를 보호하기 위해 200원을 투자할 것인가?
- 수용 가능한 목표 위험수준(DoA/Degree of Assurance) 설정해야 함

출처: 위험관리 가이드 / KISA

다음 중 보안 담당자가 수용할 수 있는 위험은?

- 게시판 없는 회사 제품용 웹페이지

  - 탈취 할만한 정보가 없는데?.. 보안 솔루션 투입하여 차단?

- 크롤러에 의한 지능적인 이미지 요청으로 인프라 부담

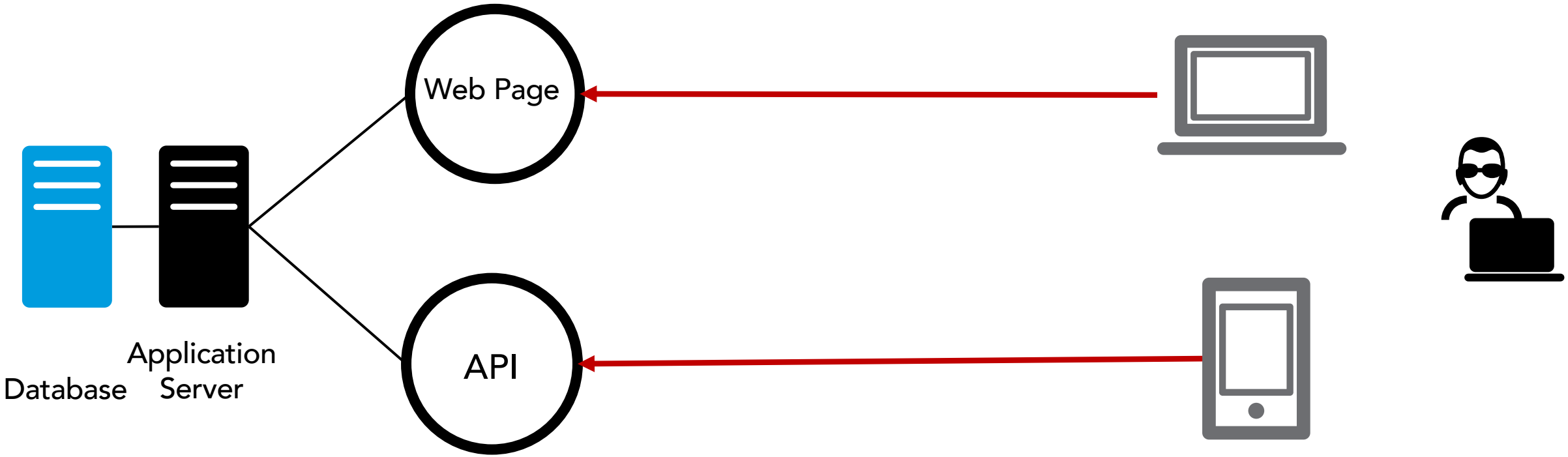
  - 인프라 추가 구매/임대 권고?.. 보안 솔루션 투입하여 차단?

- Latency 감소를 위한 웹서비스 레이어 최소화

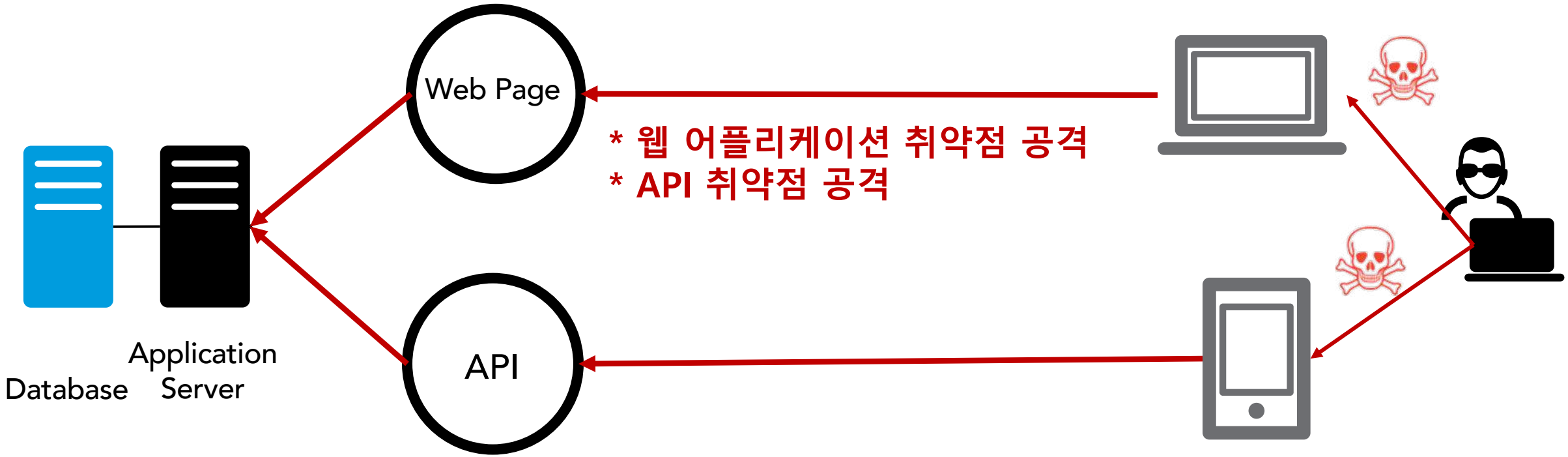
  – 성능과 보안은 반비례 관계. 보안솔루션 투입 필요?

웹어플리케이션 아키텍쳐 – 공격 예상 지점

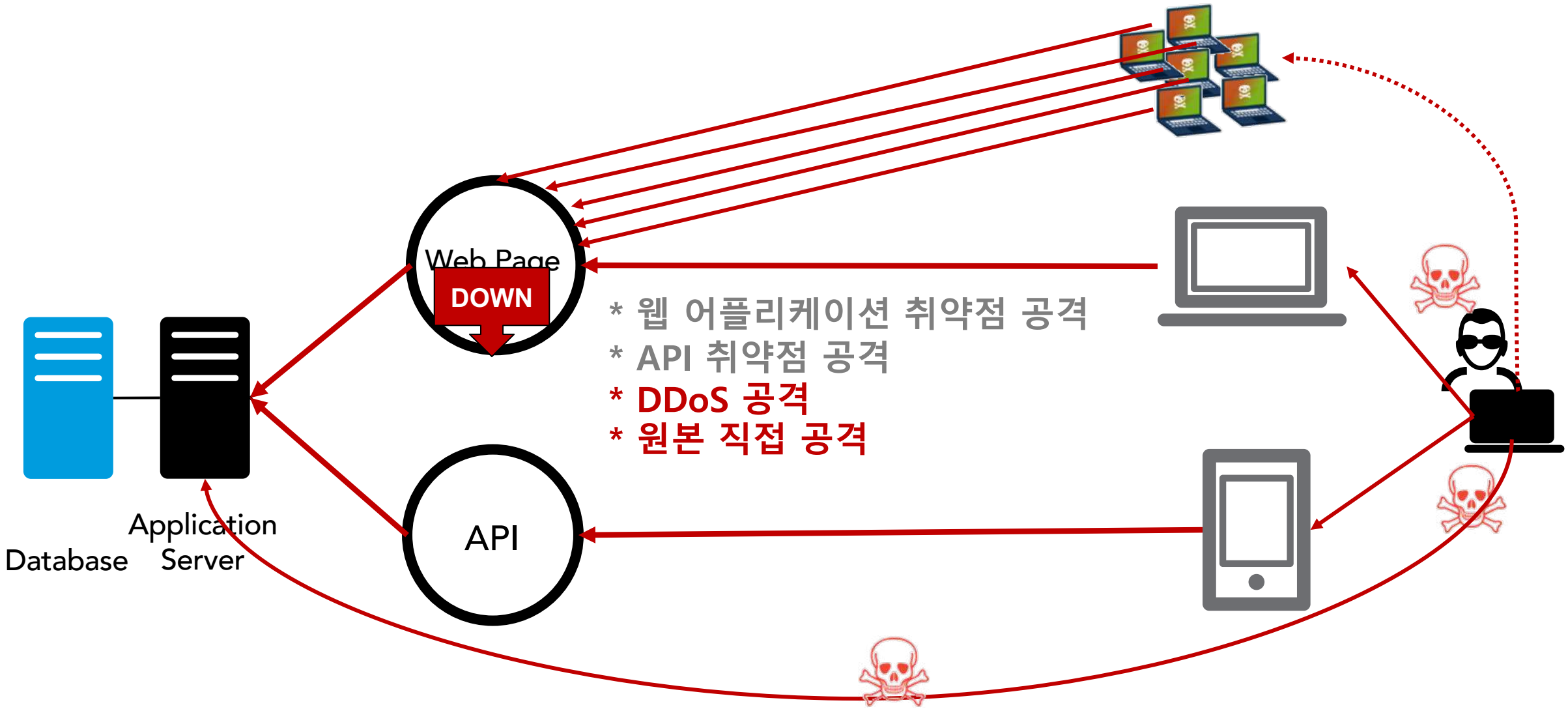
웹 어플리케이션 아키텍쳐



웹 어플리케이션 아키텍쳐

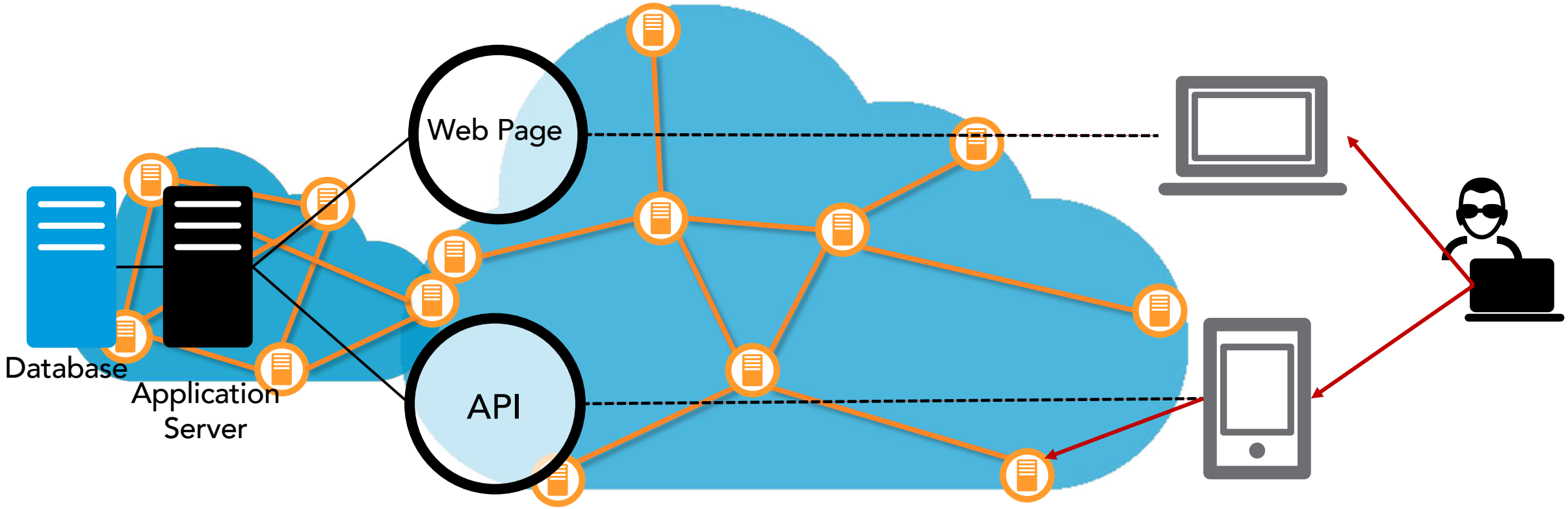


웹 어플리케이션 아키텍쳐

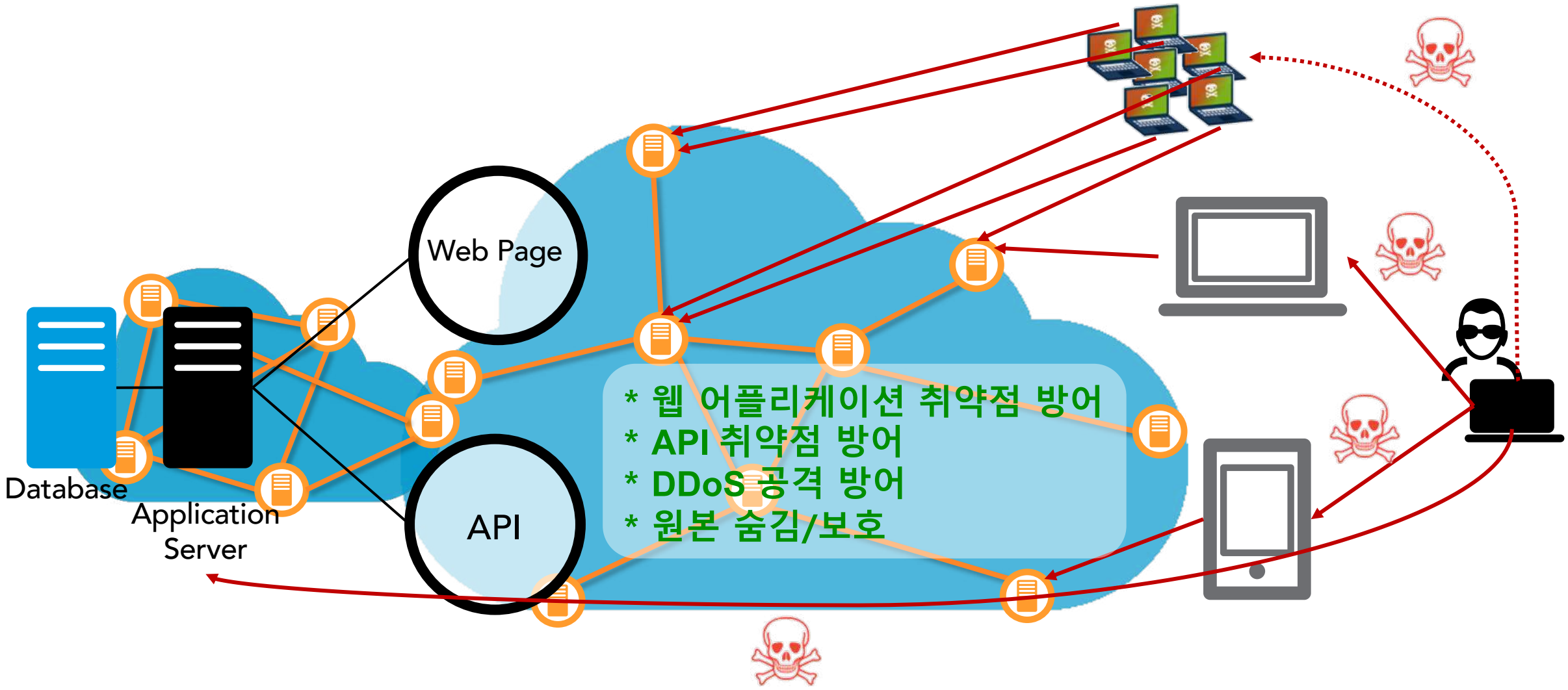


클라우드 웹방화벽 기반의 완벽한 보안 아키텍쳐

클라우드 웹 방화벽을 이용한 보안 아키텍쳐

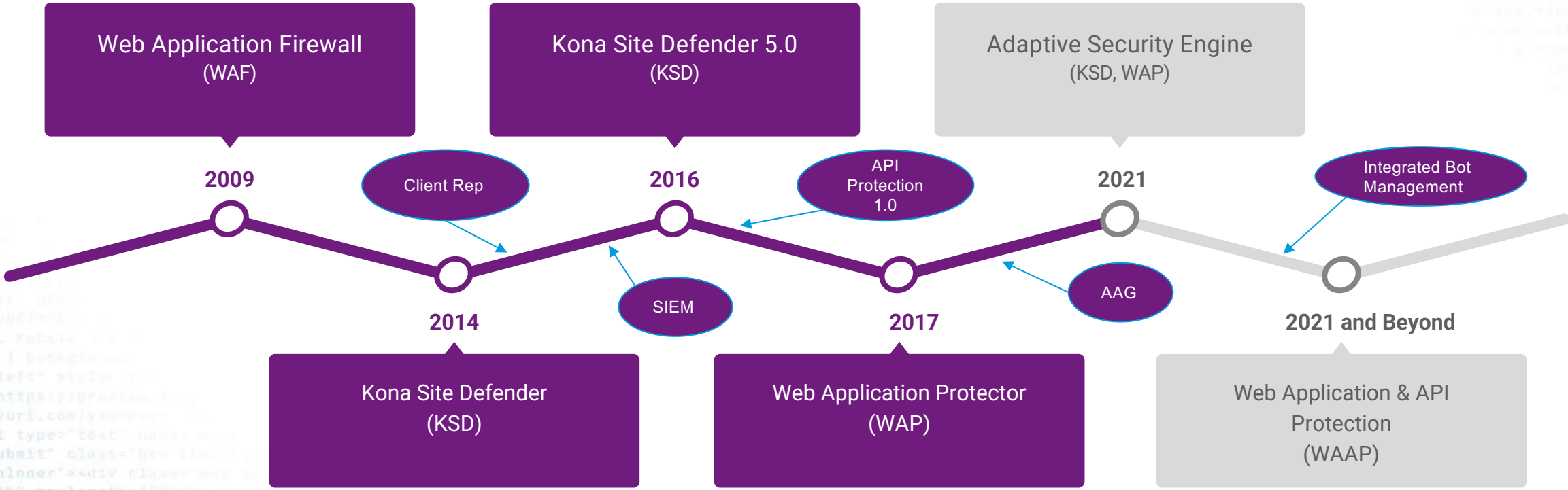


클라우드 웹 방화벽을 이용한 보안 아키텍쳐



Akamai
– Kona Site Defender

아카마이의 웹방화벽



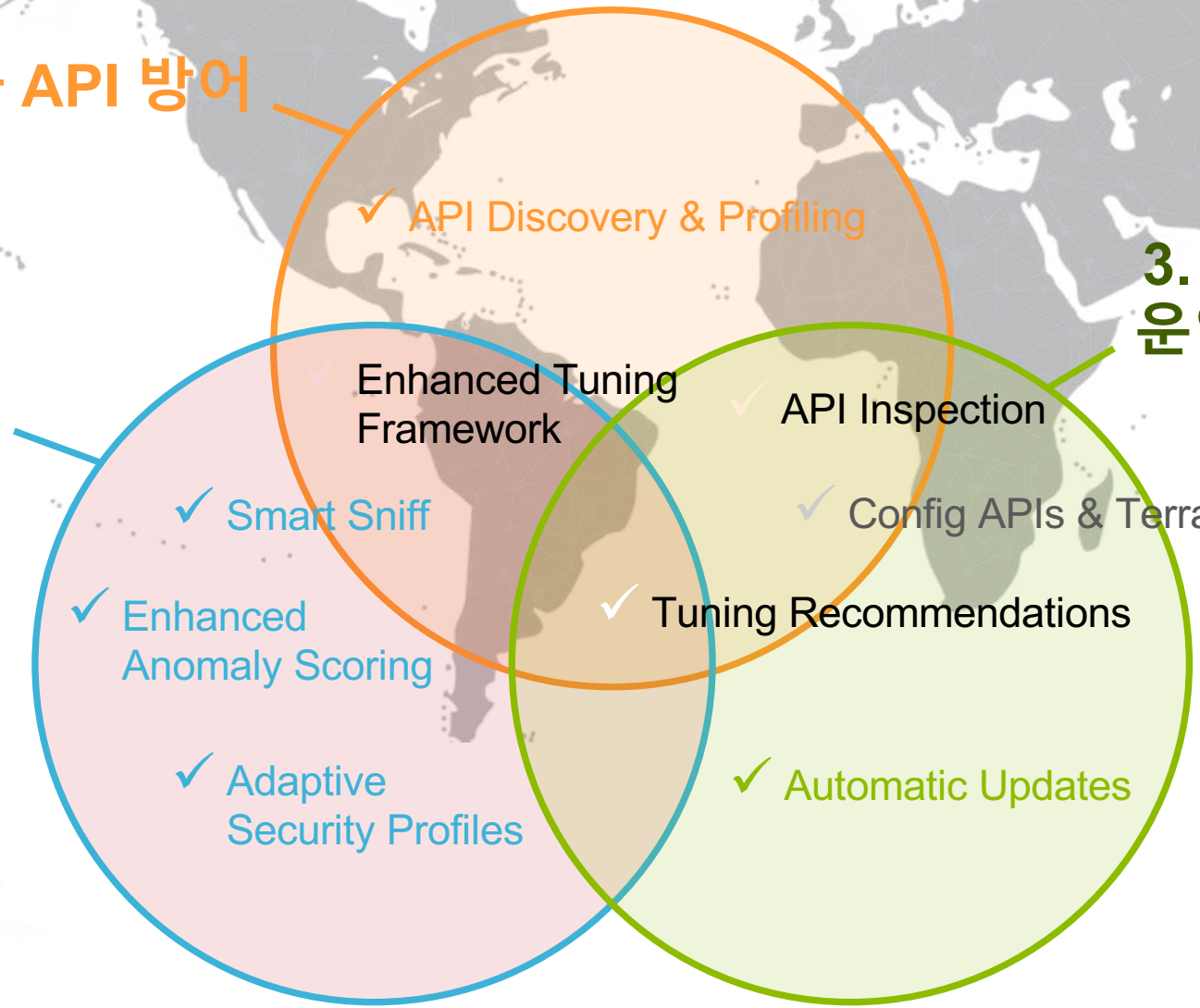
2021년 웹방화벽 기능 강화 요약

Akamai Experience the Edge

1. 웹 어플리케이션과 API 방어

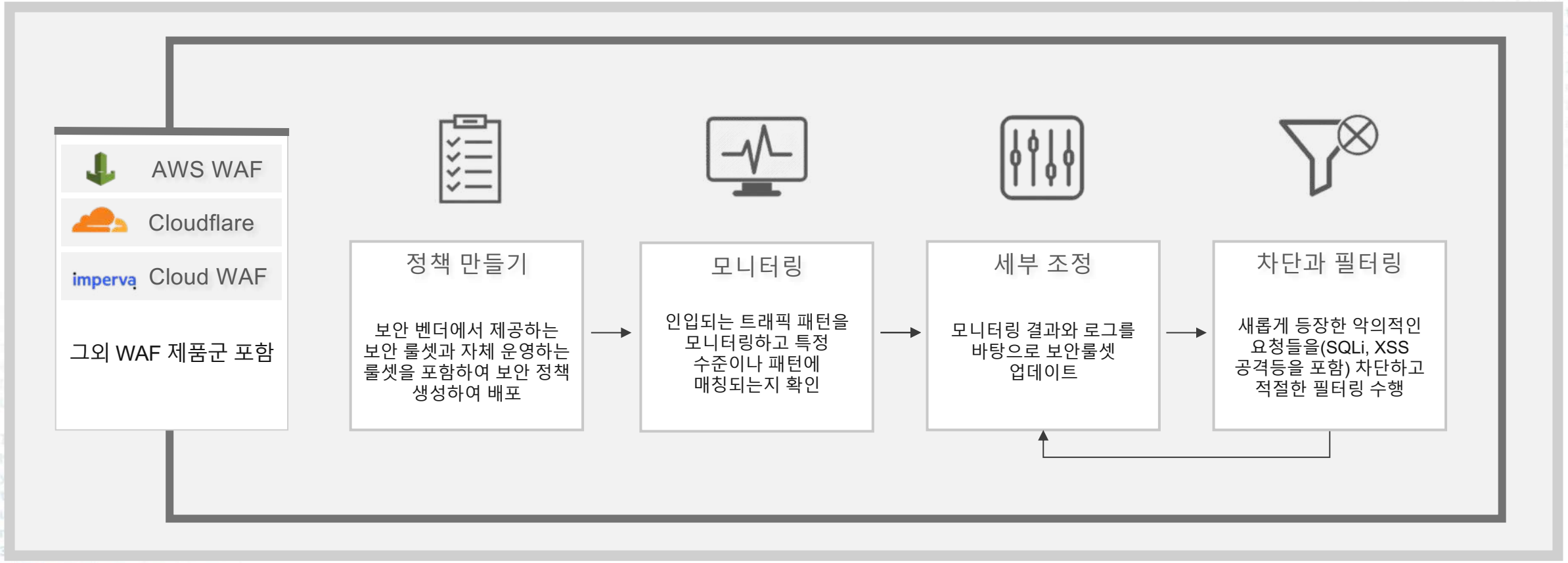
2. 오탐율 개선

3. 자동화 기반 - 비용, 운영 복잡도 감소 효과



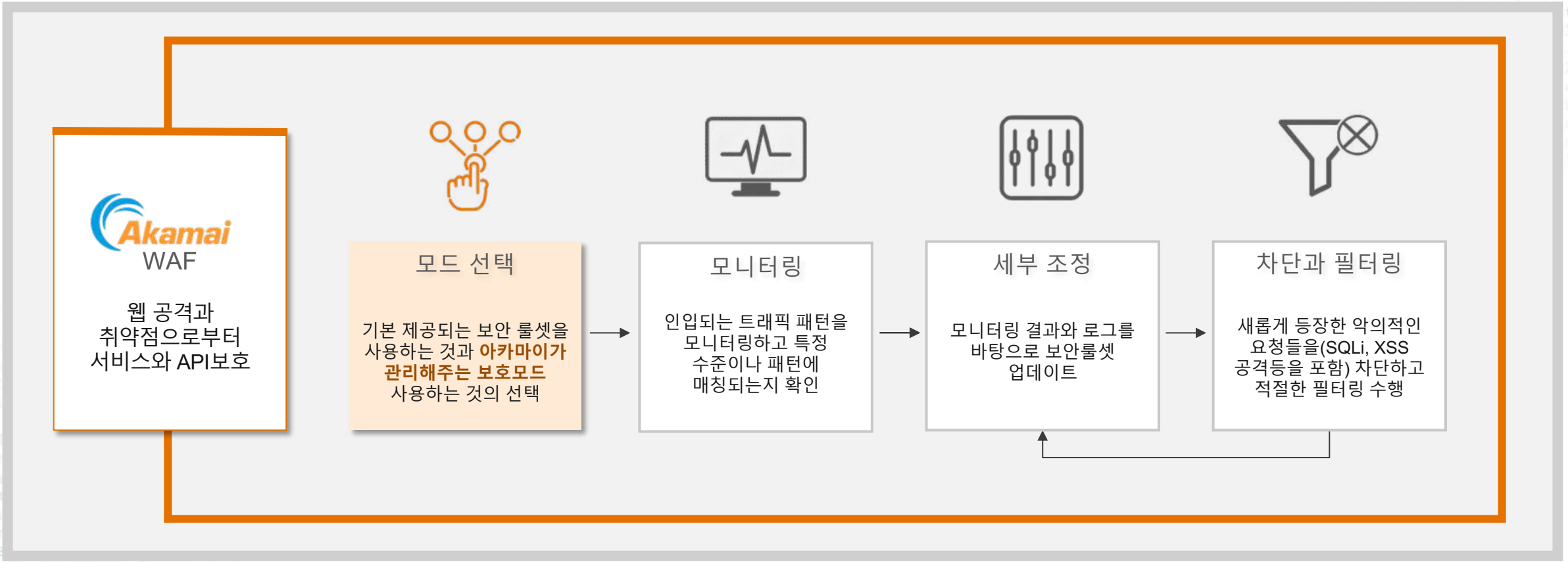
Akamai

일반적인 운영 방식



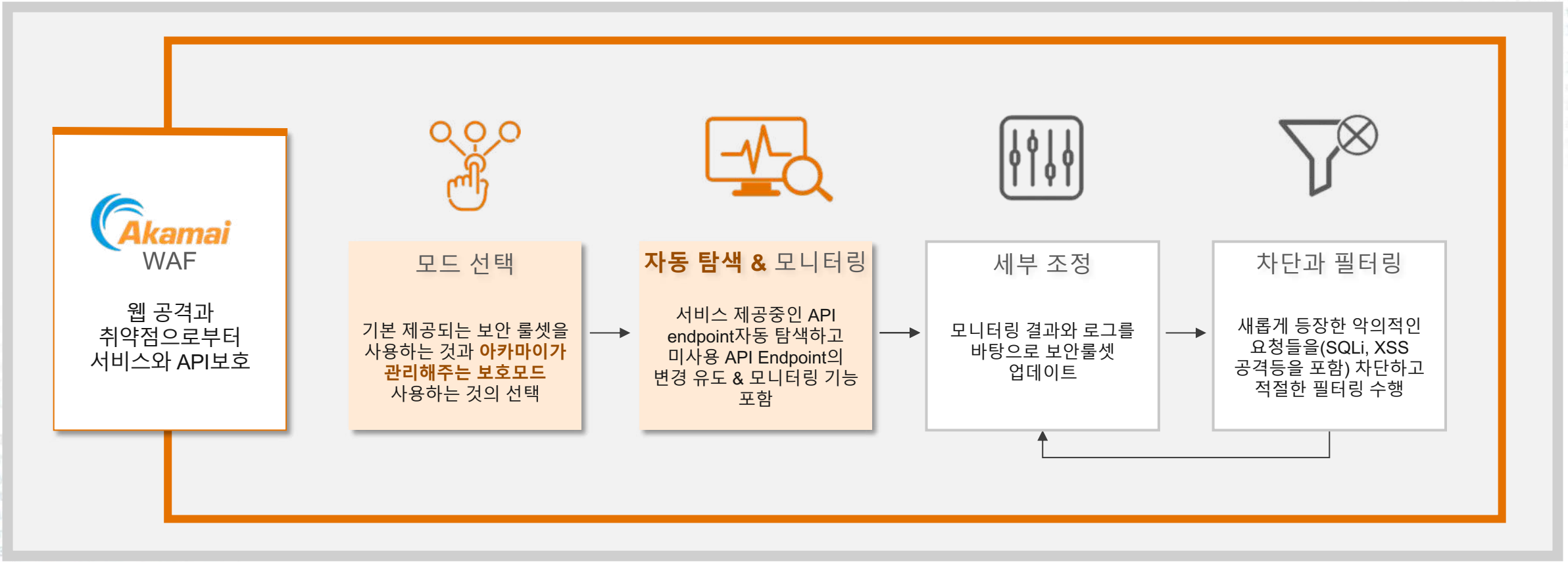
아카마이의 운영 방식 제안

AUTOMATED & FRICTIONLESS OPERATIONS



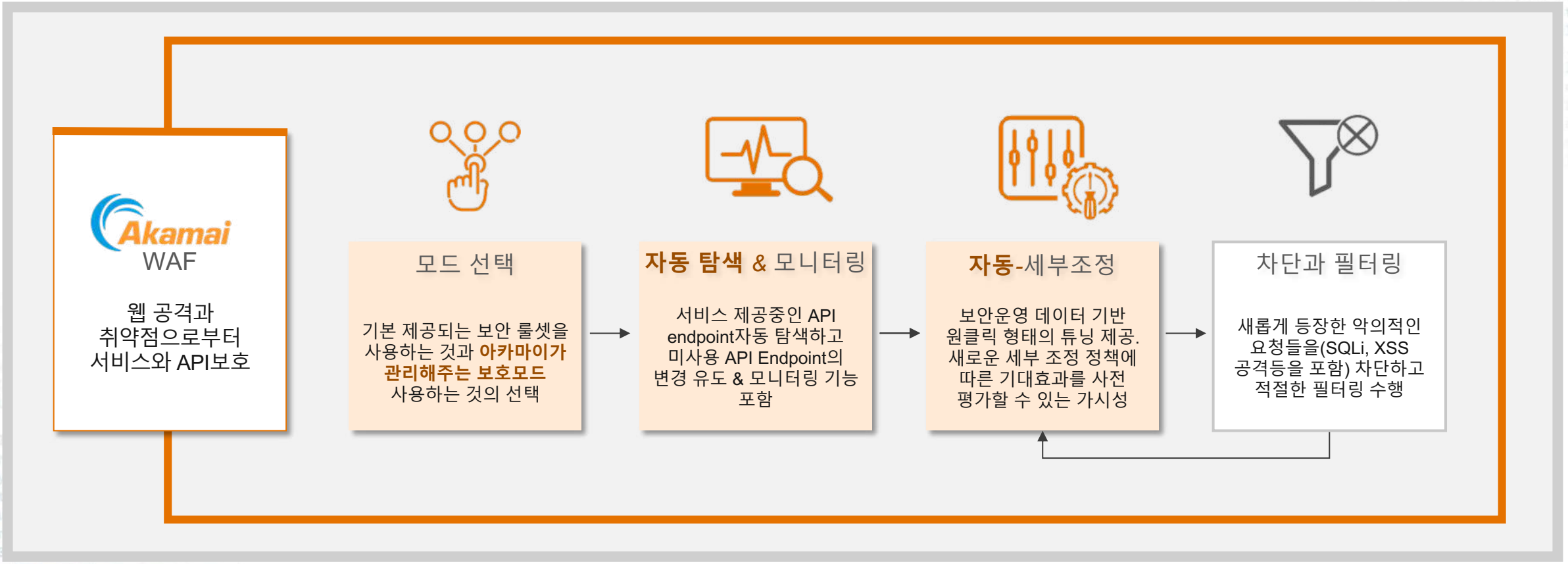
아카마이의 운영 방식 제안

AUTOMATED & FRICTIONLESS OPERATIONS



아카마이의 운영 방식 제안

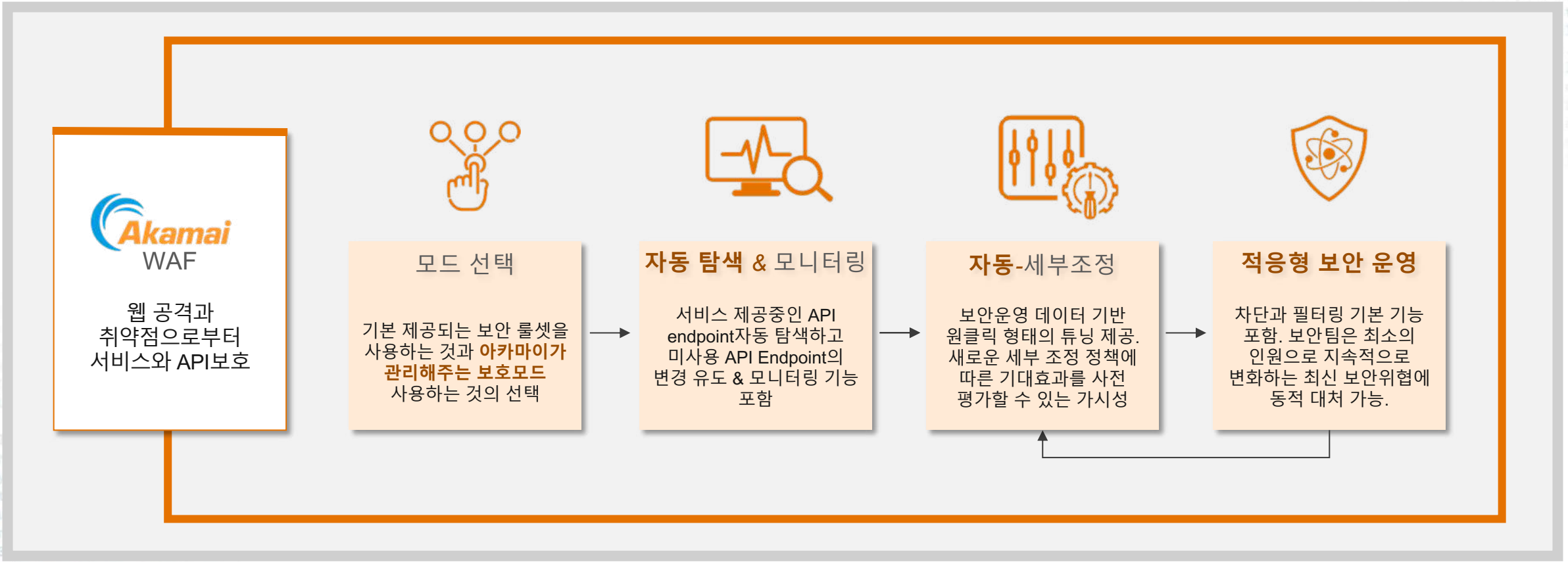
AUTOMATED & FRICTIONLESS OPERATIONS



* Q1/Q2 2021

아카마이의 운영 방식 제안

AUTOMATED & FRICTIONLESS OPERATIONS



* Q1/Q2 2021

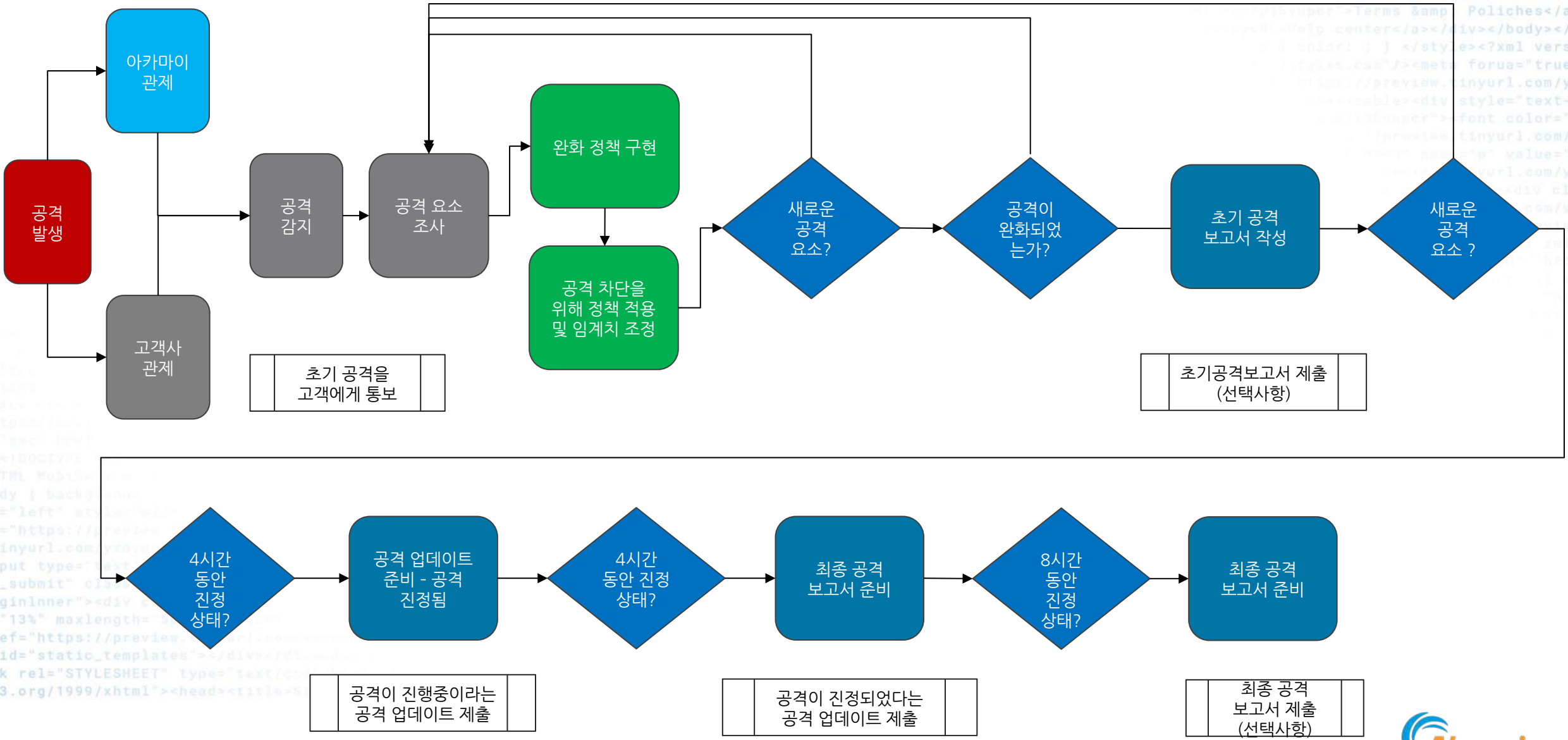
관리형 보안 서비스

보안 사고 예방 및 대응체계, 복구 대응 절차

2.11. 사고 예방 및 대응

항 목	2.11.1 사고 예방 및 대응체계 구축
인증기준	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가? • 보안관제서비스 등 외부 기관을 통해 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가? • 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?
관련 법규	• 개인정보 보호법 제34조(개인정보의 유출통지 등) • 정보통신망법 제27조의3(개인정보 유출등의 통지·신고), 제48조의3(침해사고의 신고 등), 제48조의4(침해사고의 원인분석 등)

관리형 서비스의 장점



관리형 서비스는 어디서 제공되나요?

SUPPORTS THE LARGEST SECURITY INFRASTRUCTURE IN THE WORLD

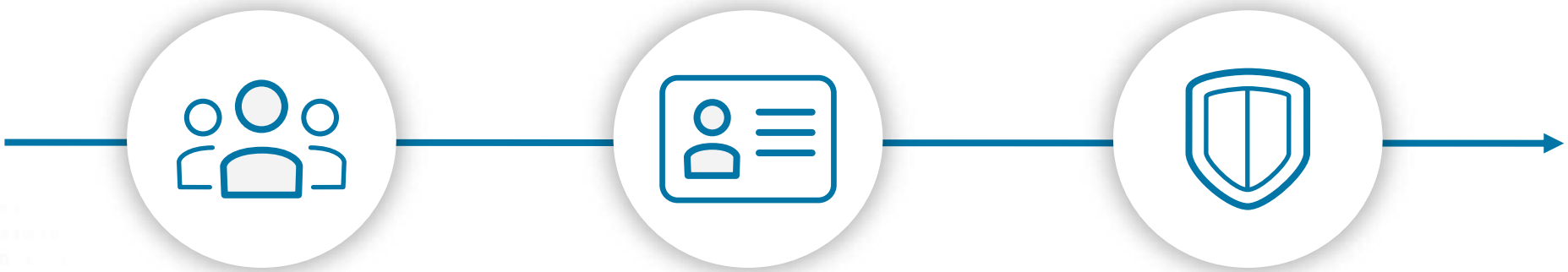
6
Security Operations Command Centers (SOCC)

255+
Certifications

200+
Security Professionals Working Overlapping Shifts

11.5K
Attacks Mitigated Annually

관리형 보안 서비스 레벨



PEOPLE

Highly trained security teams **engaged and aligned** to the customer business

EXPERTISE

Experts who know **everything** about Akamai security solutions

SECURITY OPS

Most sophisticated threat detection tech, defined security processes, best practices, etc.

MSS

Combines **security expertise** with **strong security operations**, allowing visibility and intelligence into traffic, incident response, configuration updates, and advisory reporting

Gartner Magic Quadrant 리포트

Industry Leadership

Web Application Firewalls, 2020

Figure 1: Magic Quadrant for Web Application Firewalls

Source: Gartner (October 2020)

Gartner peerinsights customers' choice

*"We have been using the Akamai WAF solution for the past 5 years, and it has delivered **every piece of result** that we, as an organization, require to protect our assets at the edge."*
– Senior Cyber Security Engineer in the Services Industry

*"The Kona WAF SaaS has worked flawlessly for us for over four years… We boast **zero downtime** due to cyberattacks in complete contrast to our previous experience; many of our sites are attack magnets and under 24x7 attack."*
– Head of Architecture – MCIT in the Finance Industry

The Forrester Wave 리포트

Industry Leadership

DDoS Mitigation Solutions
Q1 2021

Web Application Firewalls
Q1 2020

Bot Management
Q1 2020

Zero Trust eXtended Ecosystem Providers
Q3 2020

요약

클라우드 웹방화벽의 정석

요약하면..

1. **보안 위협 요소는 언제나 우상향 그래프** – 공격의 규모와 복잡도 증가
2. 보안 담당자는 **위험수준 판단과 대비**가 필요하므로 예상되는 공격 파악, 방어 수단 준비 필요
3. 적응형 보안엔진 기반으로 보안 운영 체계를 **단순화**하면서도 **고도화**
4. **보안 전문가 그룹**에 의한 안심 운영 체계 구축

보안 전문성, 보안 노하우, 풍부한 WAF서비스 경험을 보유한 파트너와 함께