Date Placeholder: Month, Day, Year

오픈뱅킹 환경에서의 어플리케이션 보안 강화와 가시성 확보

PRESENTED BY:

신은수 이사

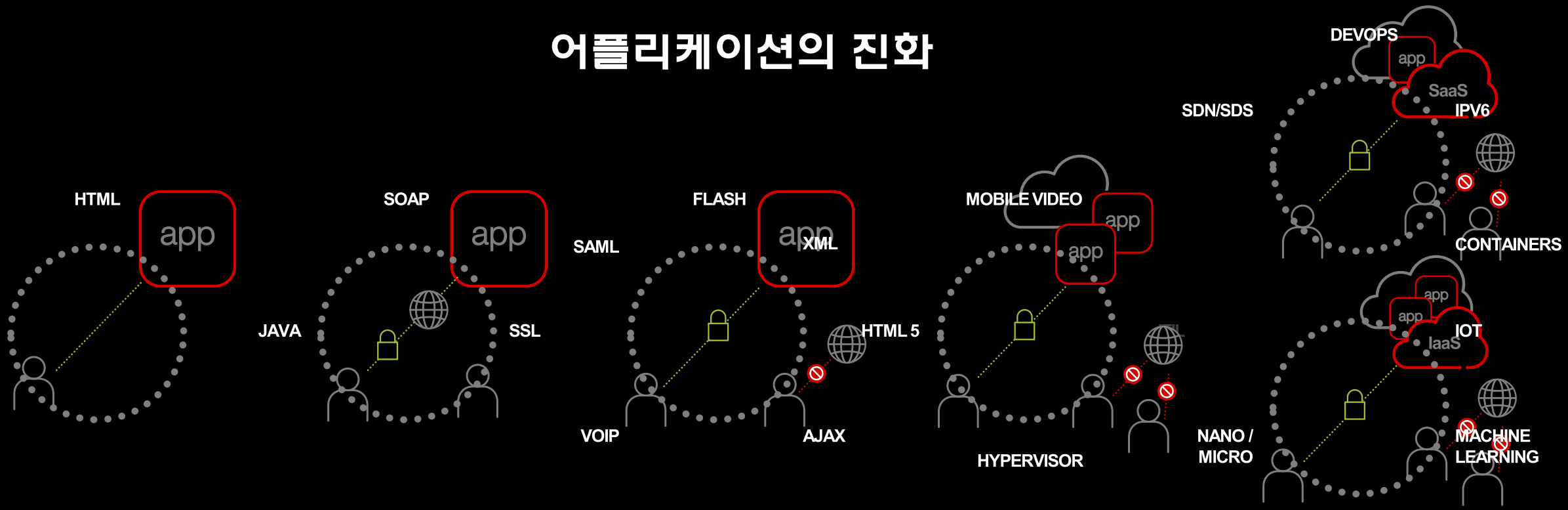
Sr. FSE

E.shin@f5.com

WE MAKE APPS GO FASTER. SMARTER. SAFER.

어플리케이션의 진화

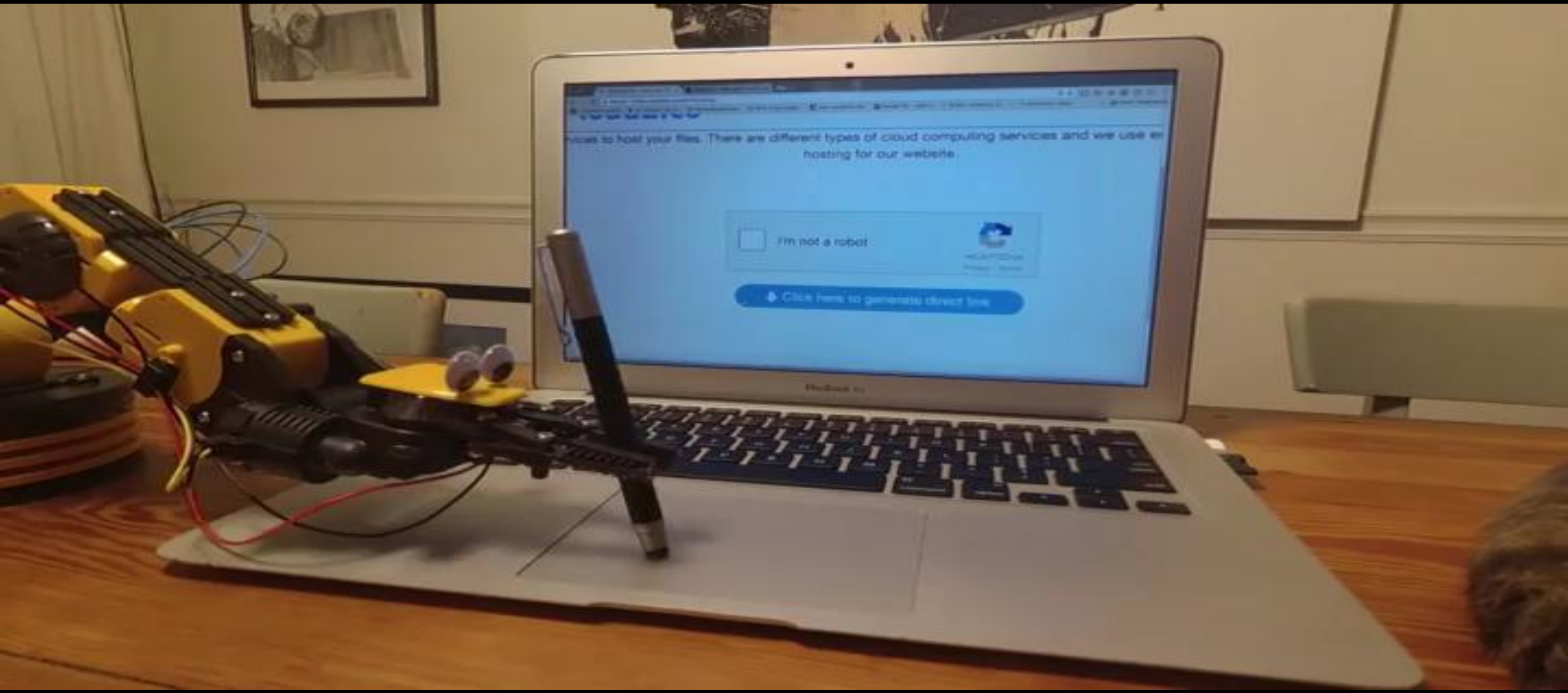
어플리케이션의 진화



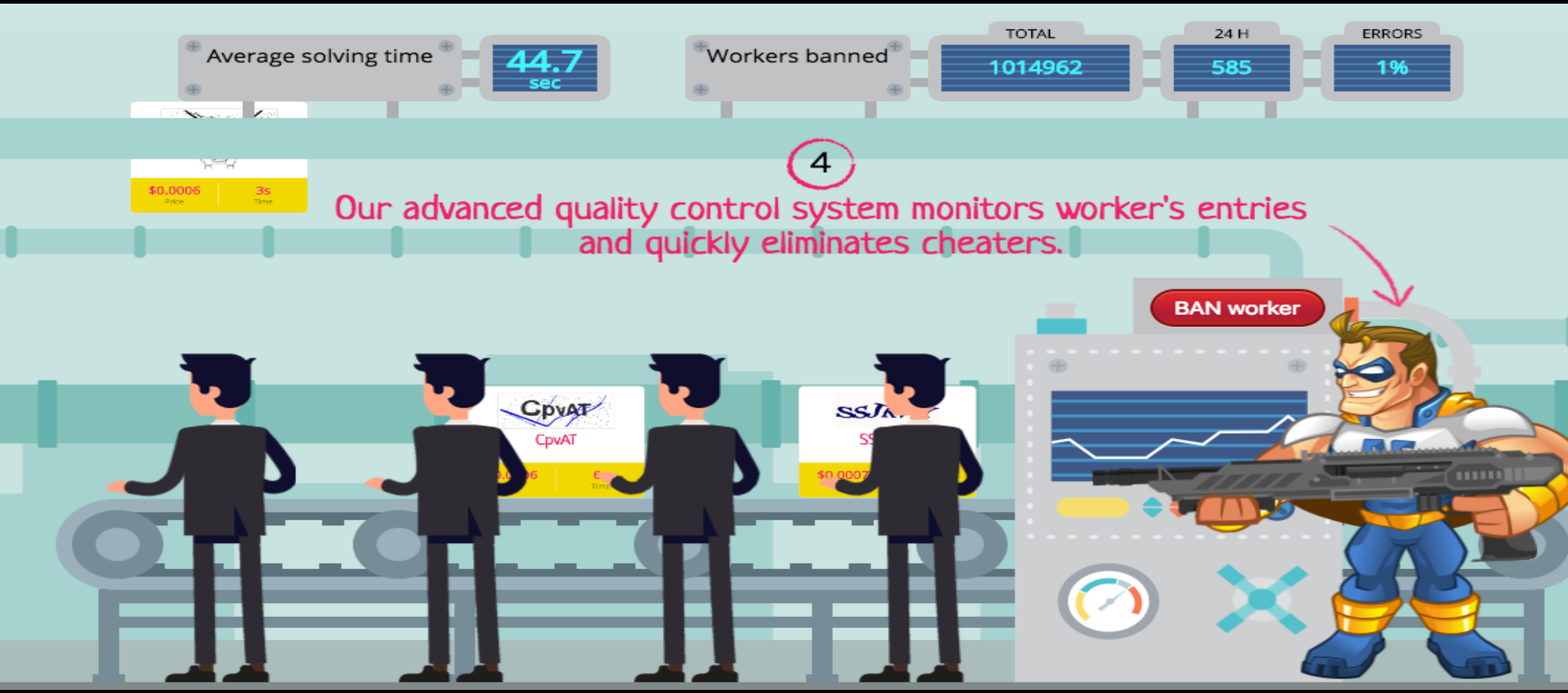
1995		2000		2005		2010		2015	
USERS	APPS	USERS	APPS	USERS	APPS	USERS	APPS	USERS	APPS
40M	20K	400M	9.5M	1B	58M	2B	207M	3.2B	1B

어플리케이션 공격

I'm not a robot



캡챠 무력화(Captcha Farm)



일반적인 보안 솔루션 우회 기법

공격 트래픽 정보

- Source IP
- 요청 헤더
- 요청 횟수

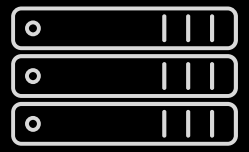
일반적인 차단 방안

- 중국 Source IP 차단(Geo DB 적용)
- User-Agent 등의 패턴 기반 차단
- 임계치 기반 차단

공격자의 차단 회피 방법

- 국내 VPN 서비스 활용
- Header 정보 변조
- 다양한 세션 사용

중국 Source IP 차단



일반적인 네트워크 기반 보안 솔루션(IPS/FW) 등의 솔루션으로는 지능화된 봇 트래픽을 차단할 수 없습니다.

새로운 방식의 어플리케이션 보호

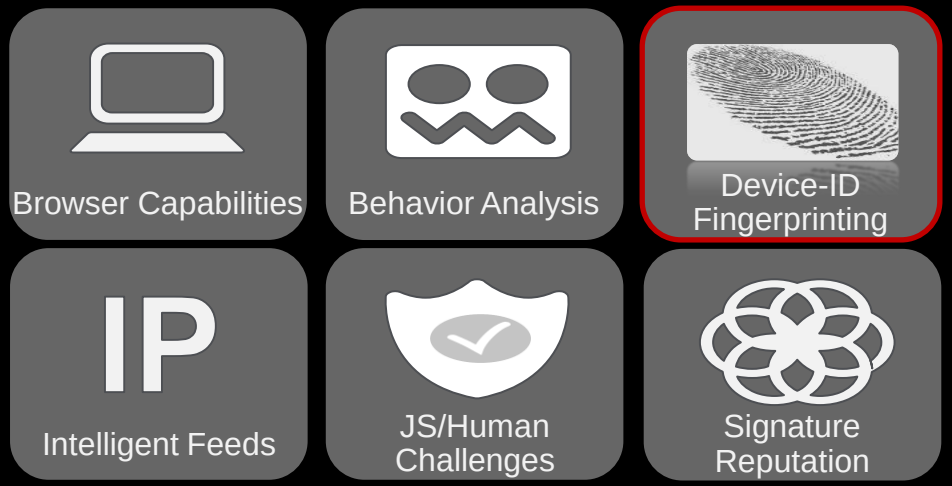
Passive – 디바이스에 대한 정보 요청 없이 진행 (ex, User-Agent, OS fingerprinting)

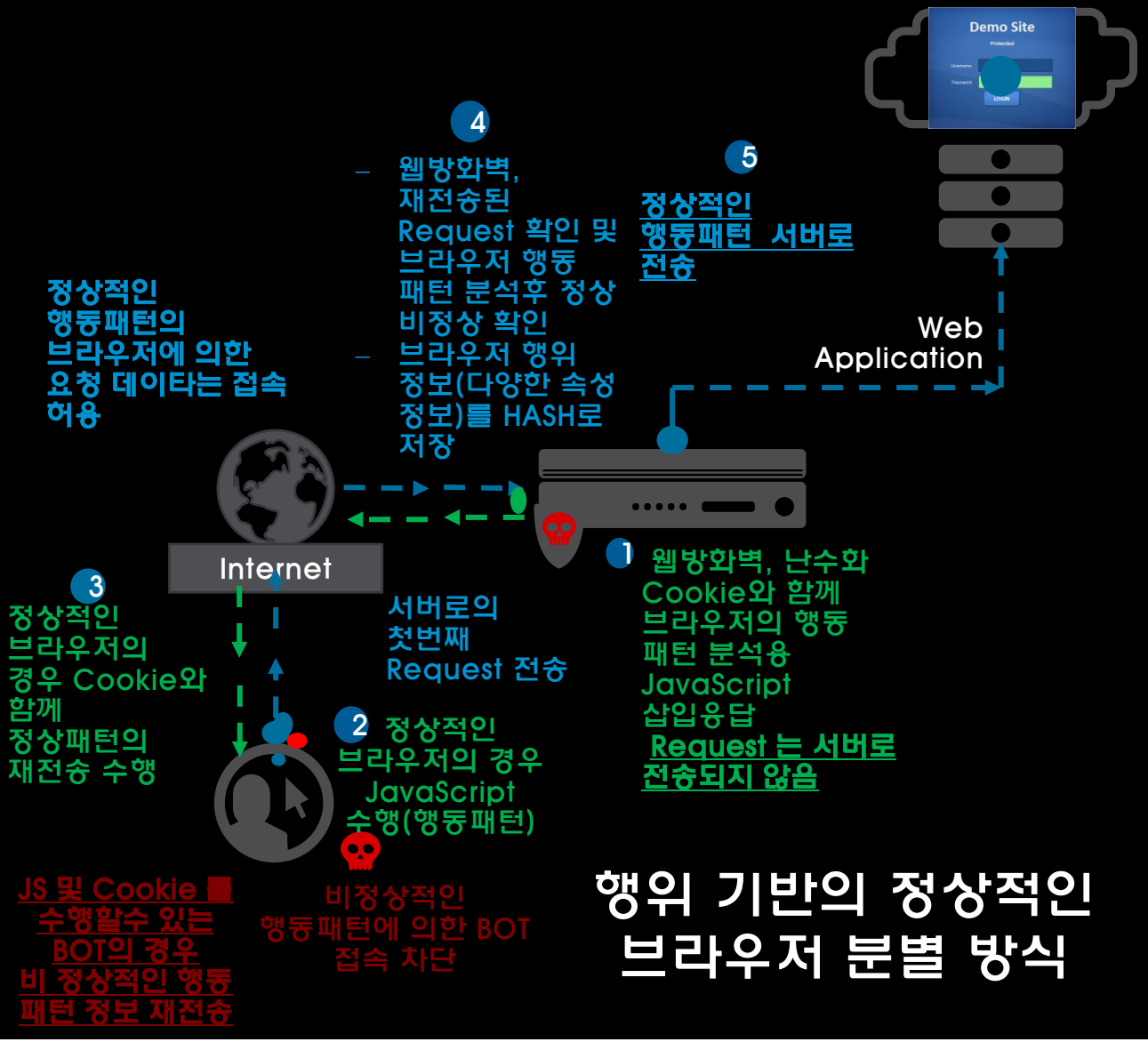
Active – JS를 통한 디바이스 분석 (ex, Panopticlick, Am I unique)

새로운 방식의 어플리케이션 보호

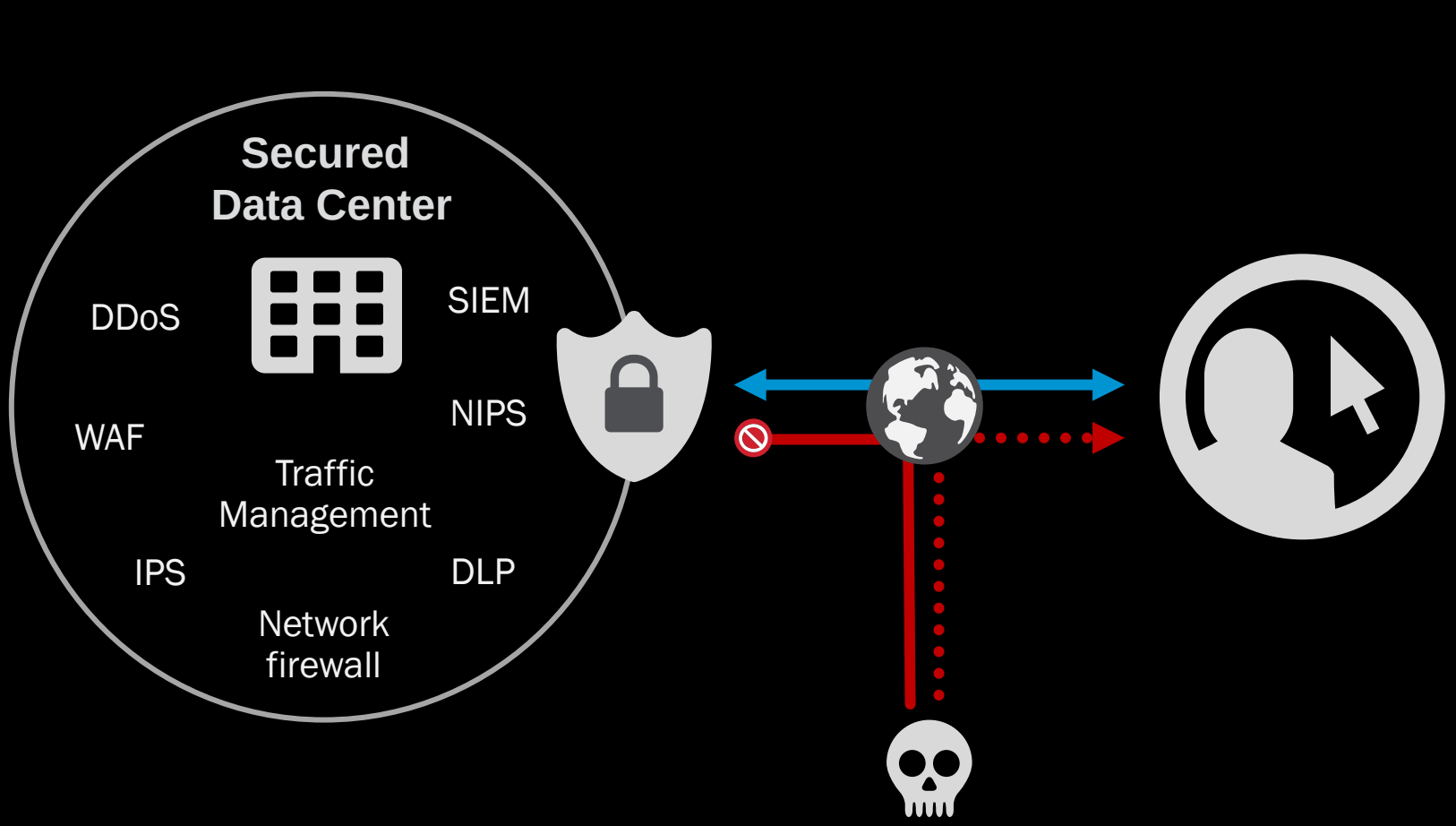
차별화된 차단 방식

- **클라이언트 단 정상 유무 확인 동작 수행**
  (접속자 정보 수집을 위한 client-side code 수행)
- **해커 정보를 해쉬 값으로 저장**
  (20+ 이상의 Unique Device 성질과 속성(i.e. 그래픽 어댑터 행위 정보) 정보를 Hash값으로 저장 (*fingerprint*).
- **저장된 정보를 통해 행위분석 수행**



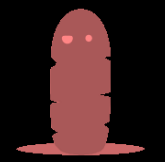


새로운 방식의 어플리케이션 보호



- Man in the Browser
- 데이터 탈취

- 피싱
- 계정 탈취

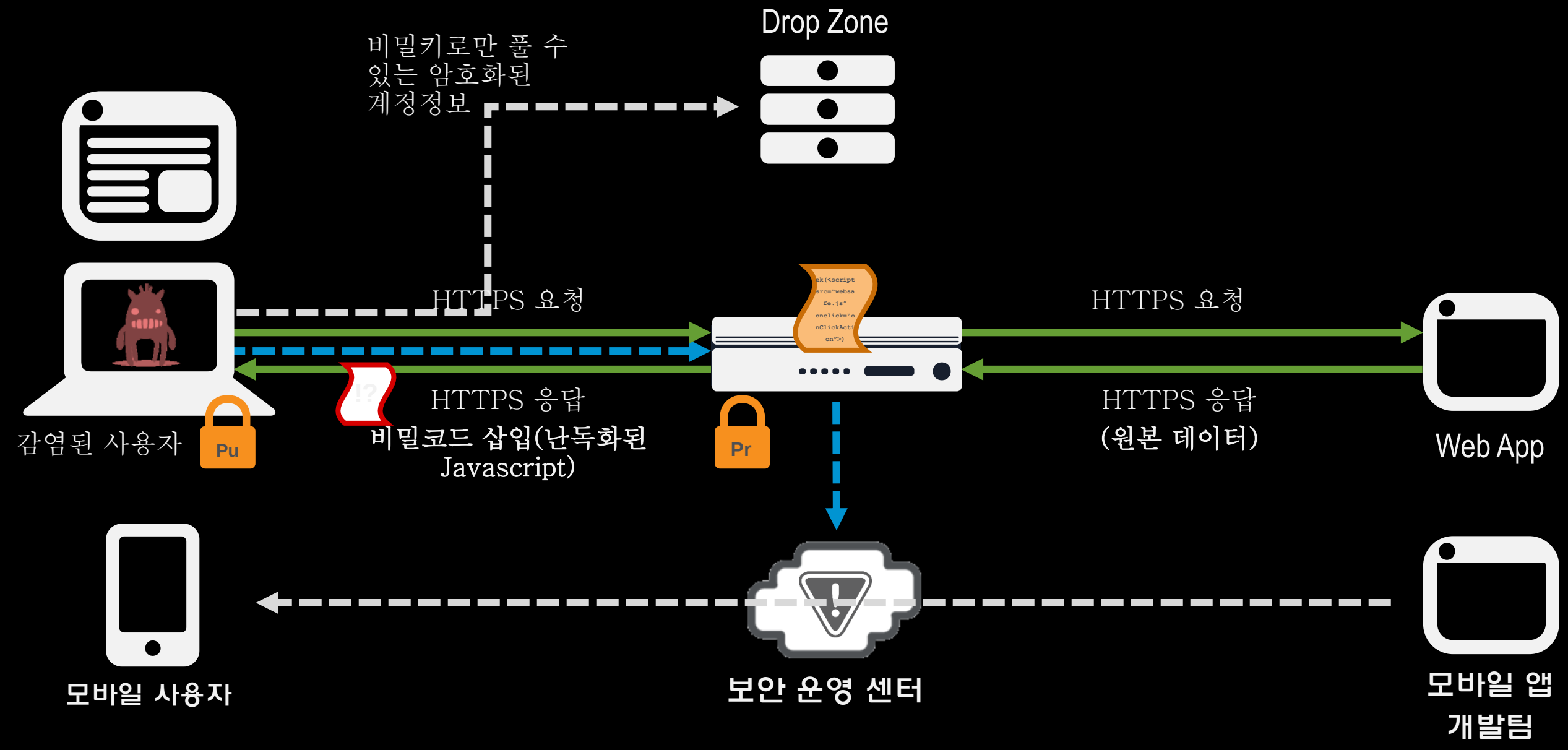


- 브라우저 캐시
- 브라우저 애드온

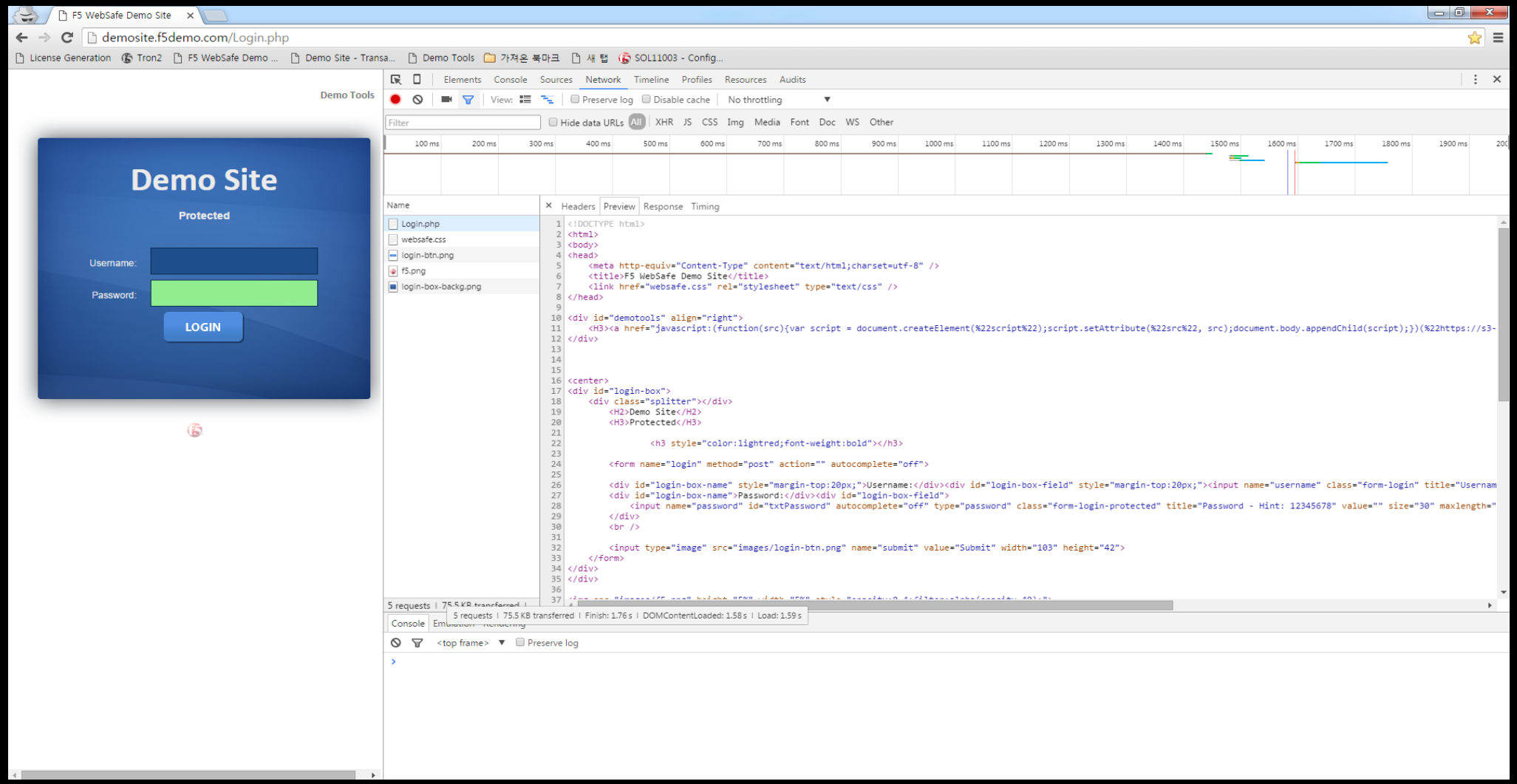
- 키로거
- 프레임 그래버

- 자동 실행 트랜잭션
- 원격제어

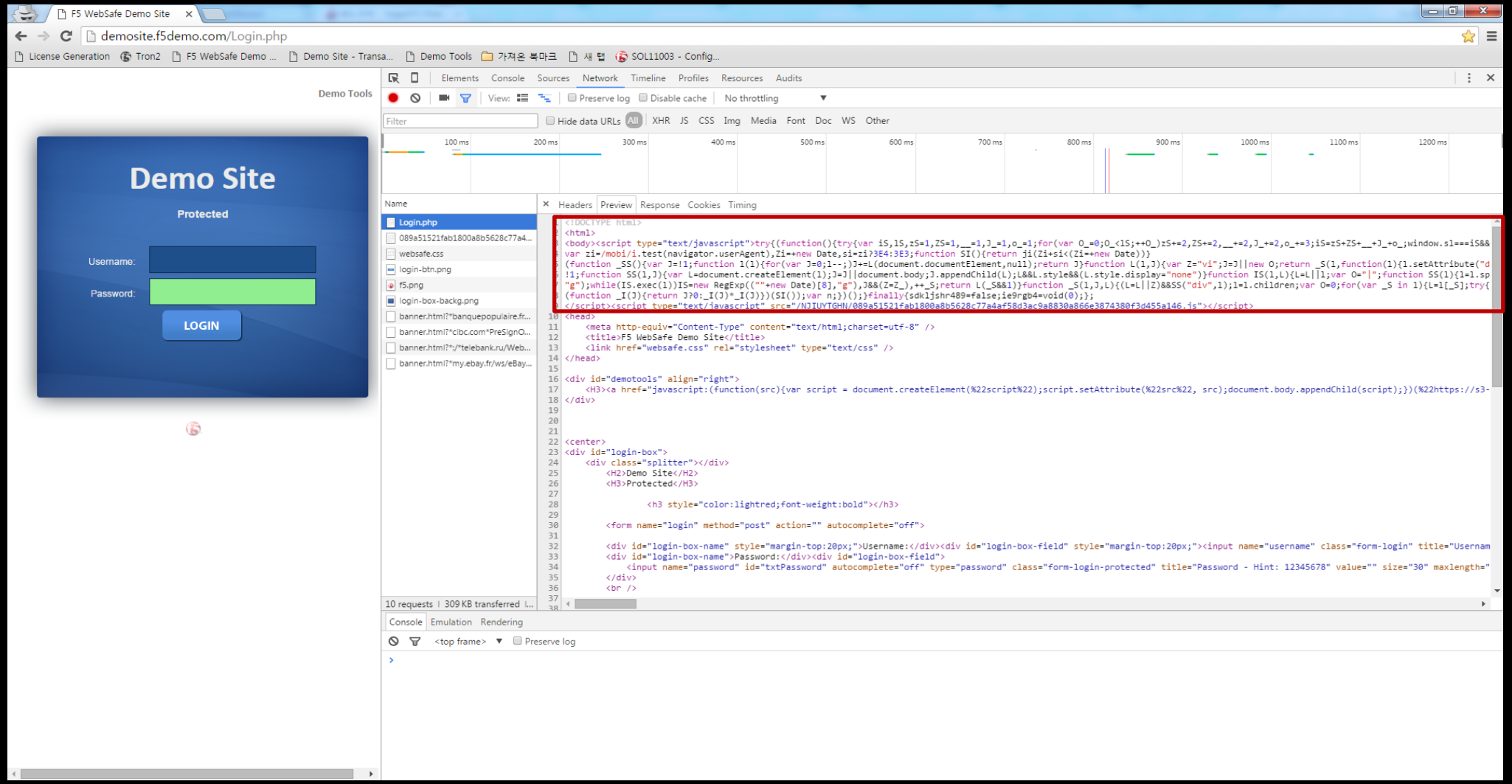
F5 Data Safe 솔루션



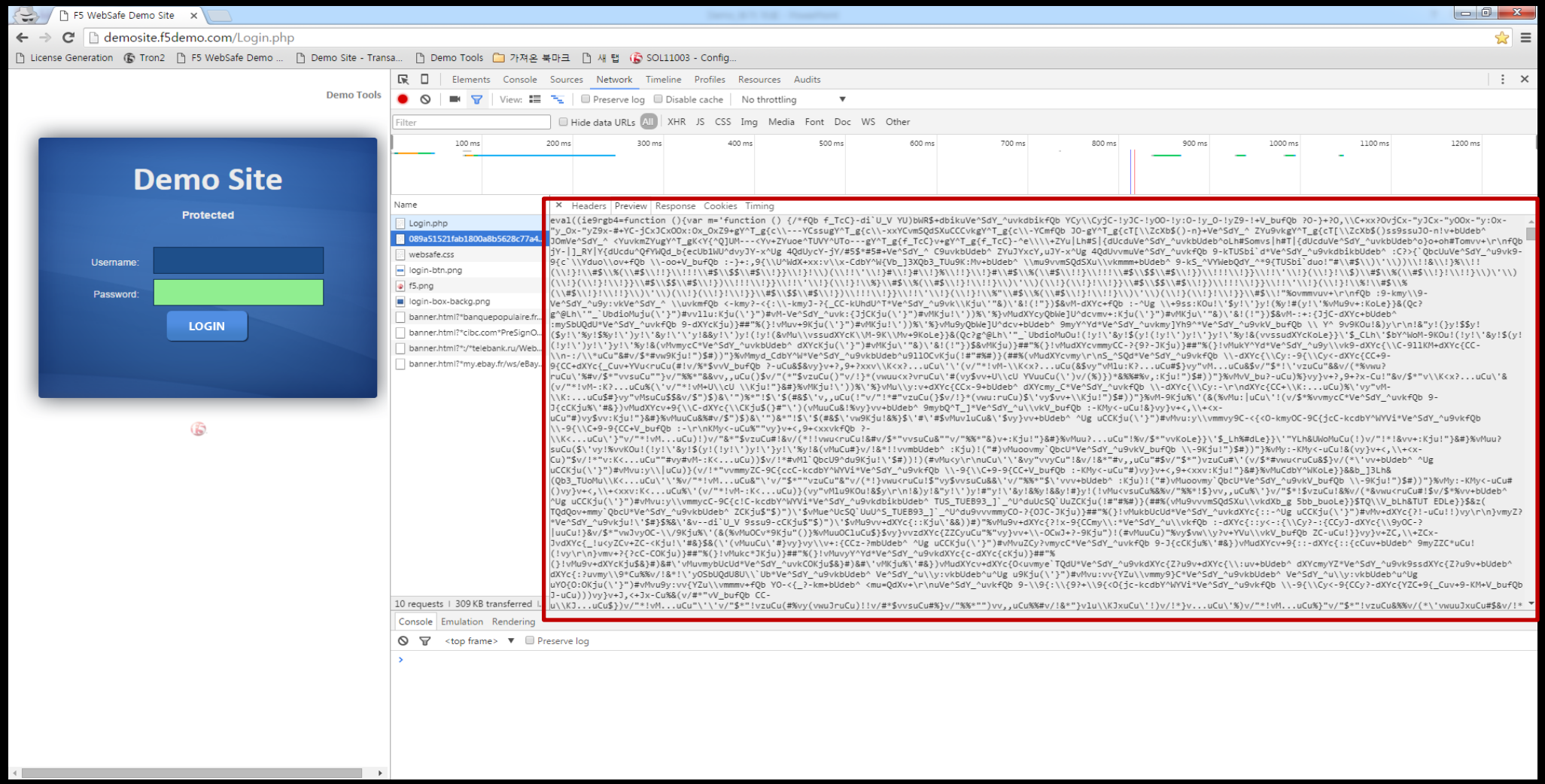
Agentless 사용자 보안



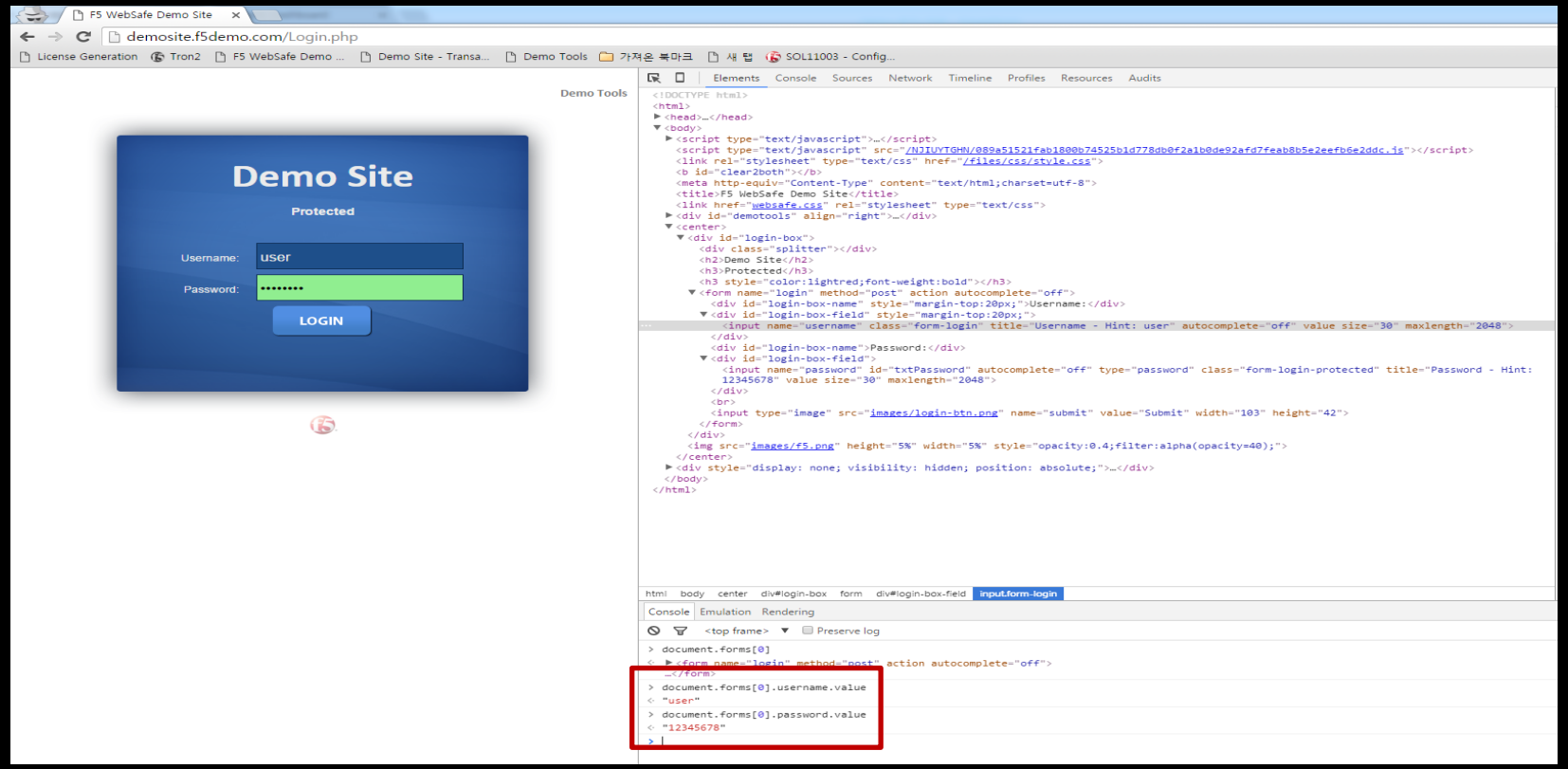
Agentless 사용자 보안



Agentless 사용자 보안

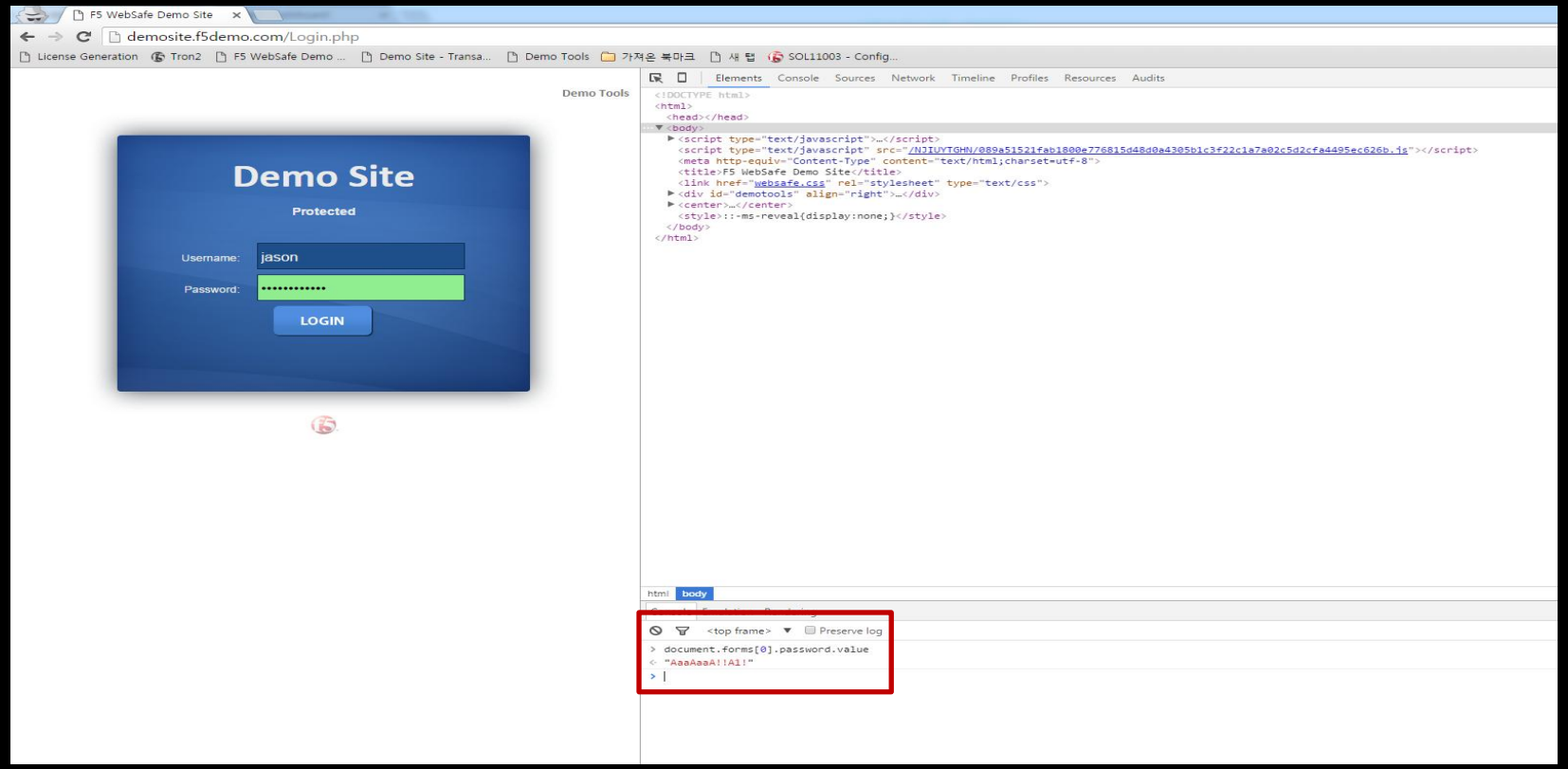


Agentless 사용자 보안 – 개인정보 암호화/치환



- 사용자가 Login 버튼을 누르지 않은 상태에서도 공격자는 멜웨어를 이용하여 사용자 고유 정보 ID / Password를 갈취해 갈 수 있음

Agentless 사용자 보안 – 개인정보 암호화/치환



- F5 Application Layer Encryption 기능은 대문자: A, 소문자: a, 숫자:1, 심볼:!로 자동으로 변경
- 공격자는 치환된 패스워드를 이용하여 접속 시 Login 불가 및 알람 발생

SSL 가시성 확보

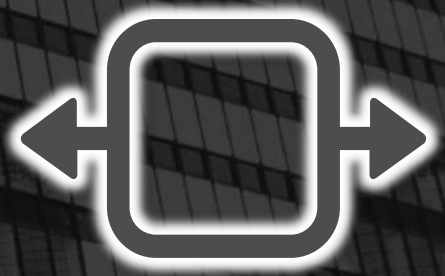
증가하는 SSL 트래픽에 대한 우리의 고민

악성코드

탐지를 피하기위해
암호화 채널을 사용

가시성

SSL사용율의 증가로 인해
가시성이 현저하게 떨어짐



성능

암호화 및 복호화는 현저한
성능감소로 이어짐

SSL 가시화 솔루션을 통한 탐지/차단

SSL 가시성 제공을 통해 기존의 침해탐지 및 차단솔루션에서 SSL을 통한 악성코드 배포를 탐지 및 차단

차세대 방화벽 | DLP | 악성코드 탐지 | 보안 웹게이트웨이 | 사용자 모니터링 | 기타 보안솔루션

네트워크 모니터링 IT 인프라

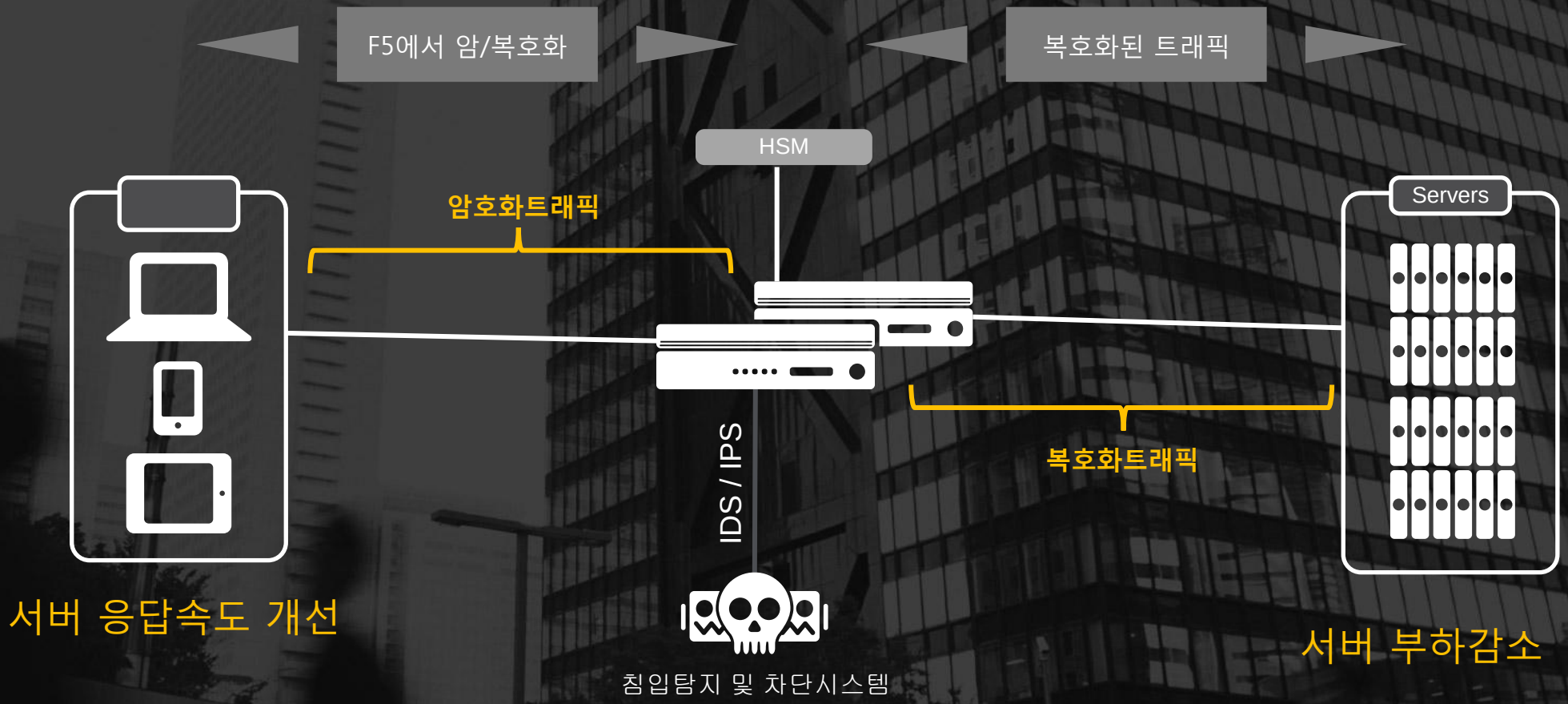
SSL 가시성 및 탐지의 종류

Reverse Proxy
오프로드/브릿지/가시성

Forward Proxy
SSL Intercept

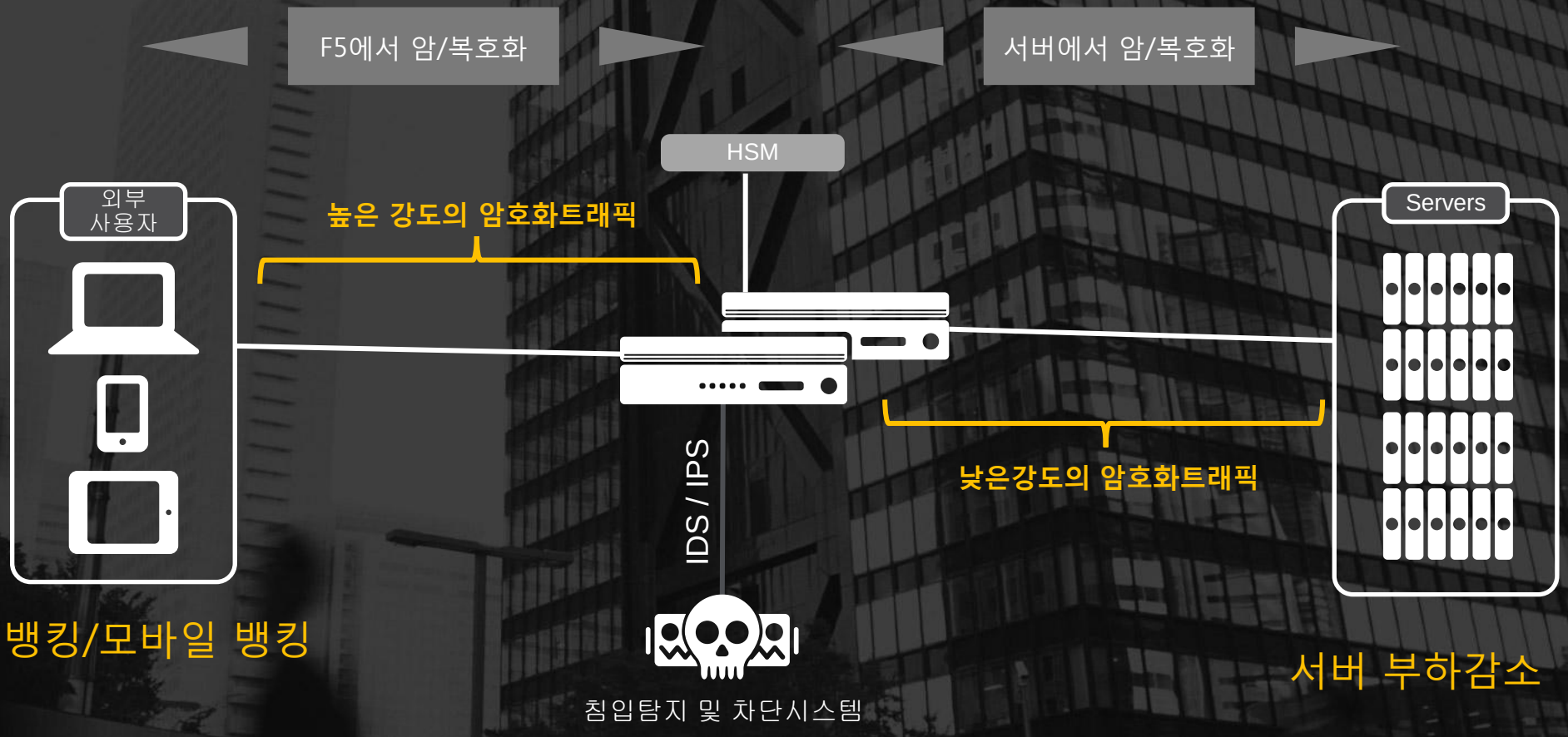
솔루션 구성방식

SSL 가속 & Offloading



보안장비 연동 및 성능개선 / IDS/IPS 효율극대화

SSL 가속(Transformation)



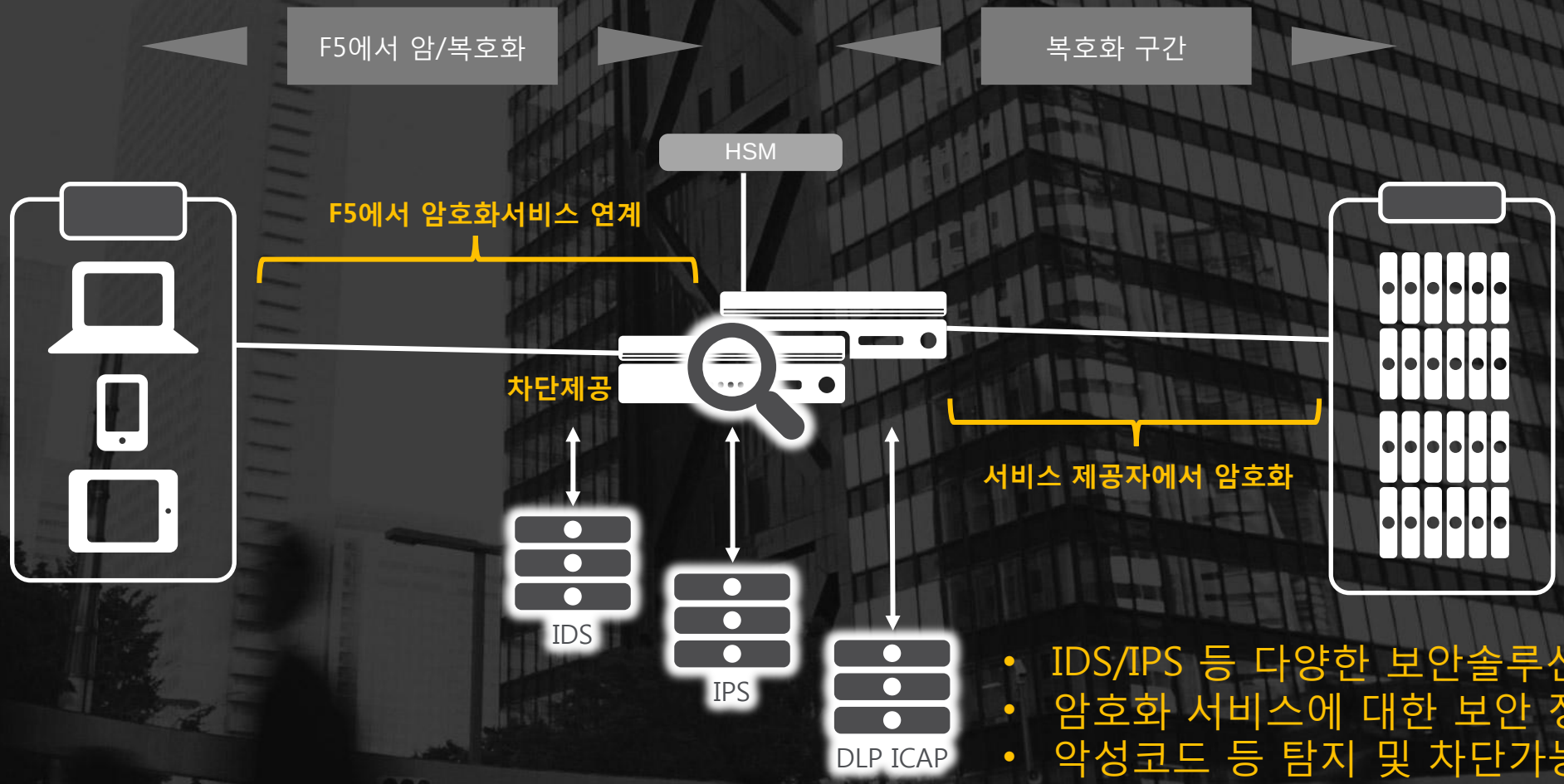
오픈 뱅킹/모바일 뱅킹

서버 부하감소

침입탐지 및 차단시스템

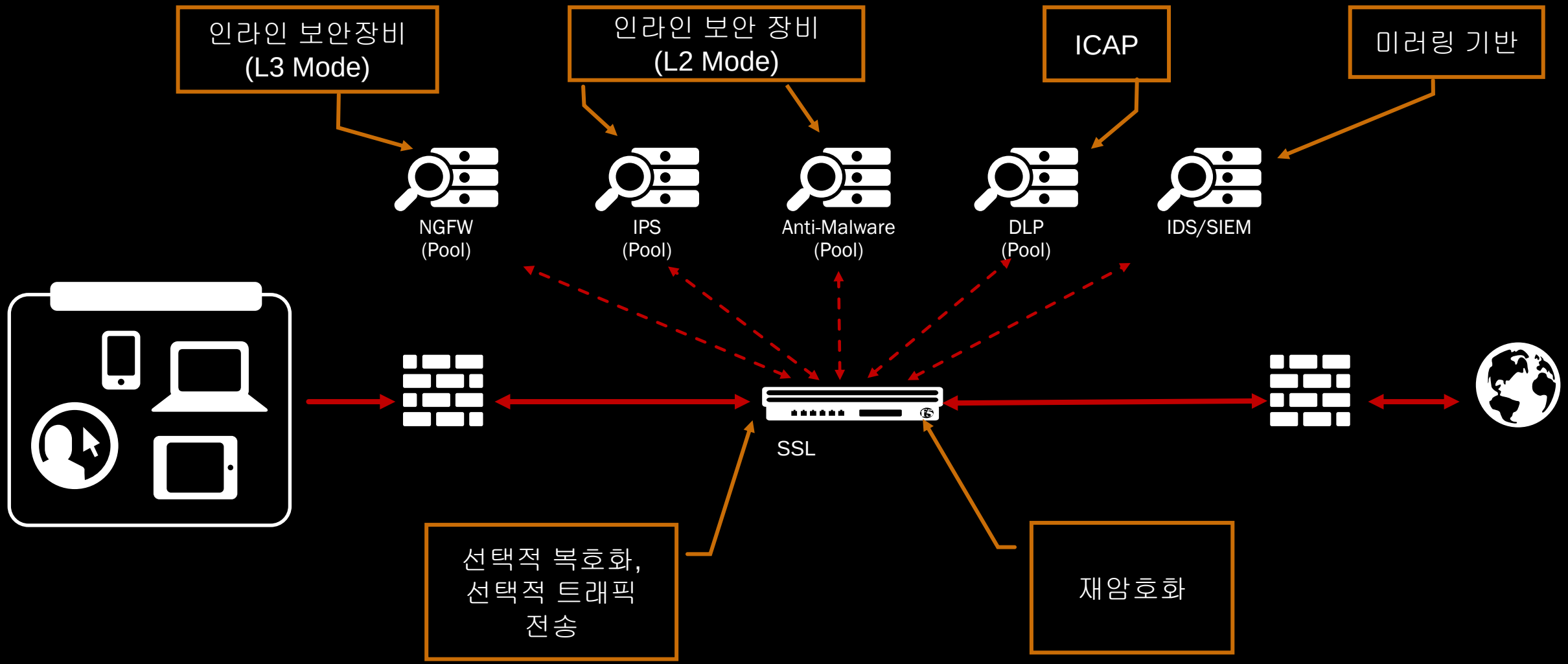
IDS/IPS 효율극대화

SSL Reverse Proxy



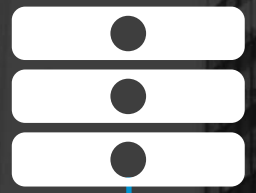
- IDS/IPS 등 다양한 보안솔루션 연계
- 암호화 서비스에 대한 보안 정책 적용
- 악성코드 등 탐지 및 차단가능

다양한 보안 솔루션과의 연동 고려



향후 SSL 가시성 확보를 위한 TOP 5 고려사항

확장성
보안솔루션 확장에 대비한
부하분산 기능



1:N 지원
다중 보안솔루션에 대해
1:N방식의 처리가 가능

Key사이즈
하드웨어 기반의 **4096 Bits** Key
처리가 가능해야 함

다양한 프로토콜 지원
ICAP프로토콜등 다양한 프로토콜을
통한 실시간 상호연동 지원

SSL 신기술 지원
SSL 트랜드 변화에 따른
ECC 알고리즘을 지원

SSL 트래픽에 대한 가시성 확보를 위해 준비된 솔루션인가? 확인하십시오!!

WE MAKE APPS

FASTER. SMARTER. SAFER.