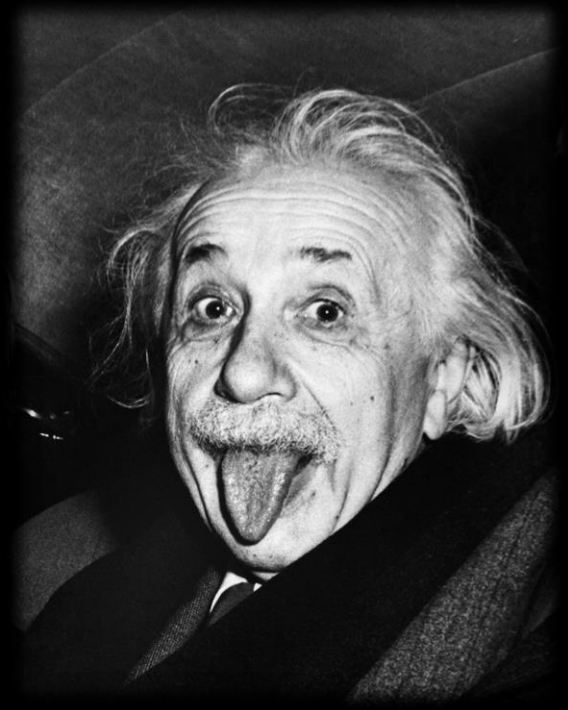
금융권 *Digitalization* 트렌드에 따른 엔드투엔드 보안 대응 전략

F5 네트웍스 코리아
보안 사업 총괄
김민영 이사 (r.kim@f5.com)



"어려움 한 가운데 그곳에 기회가 있다"

알버트 아인쉬타인
이론 물리학자(1879–1955)

증가하는
채널의 다양성

이커머스와
연계

금융 서비스
(빈도와 주기)의
양자 도약

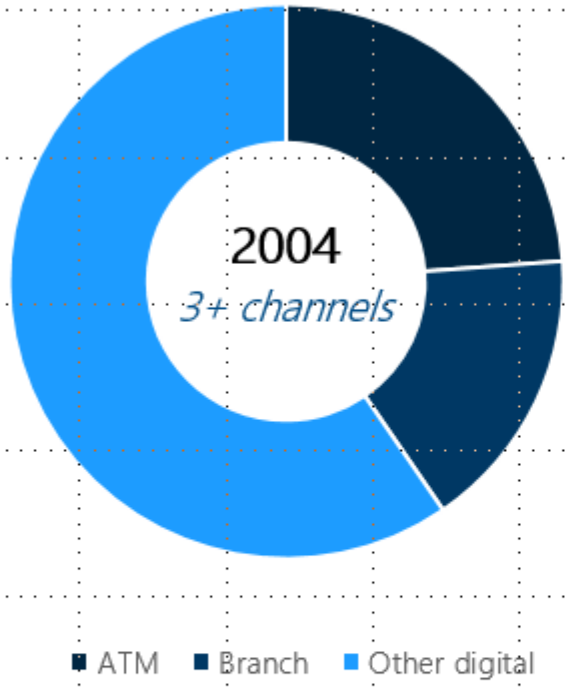
증가하는
채널의 다양성

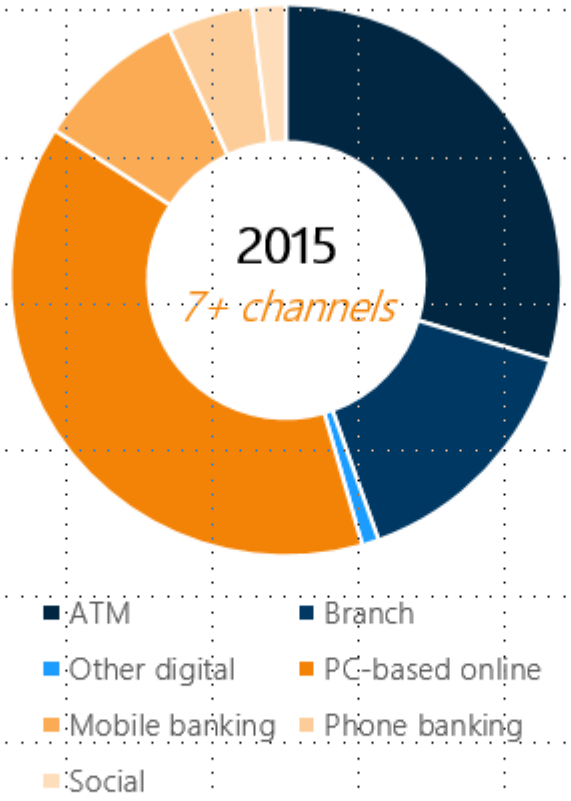
이커머스
통합

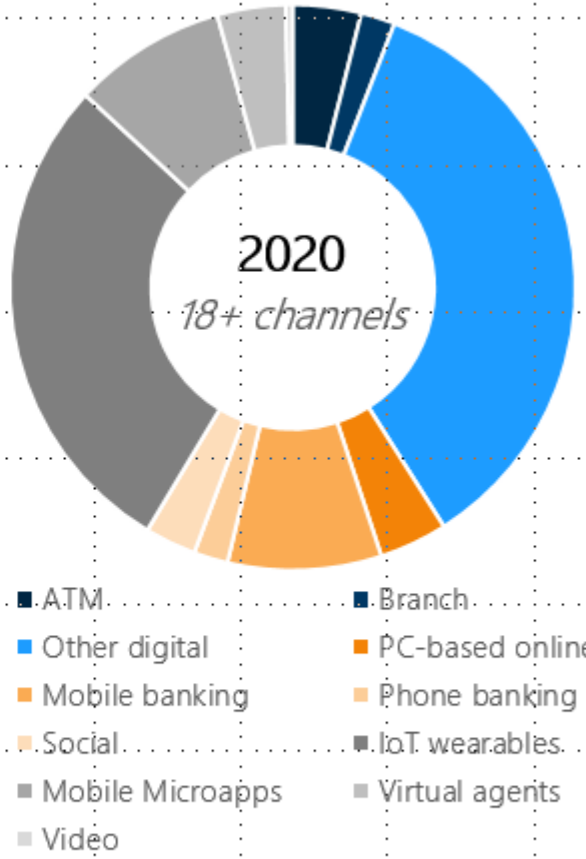
금융 서비스
(빈도와 주기)의
양자 도약

채널 다양성의 세계

은행 고객들은 이제 더 많은 채널을 통해 뱅킹거래에 참여하고 있고 – 대부분의 이러한 채널들은 2020년까지 급속한 디지털화 될 것으로 기대







IDC
Analyze the Future

IoT 디지털 기기의 보안 취약성을 말하다

…is IoT Secure?

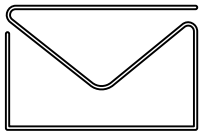
65% believe IoT is more vulnerable to attacks

66% are experiencing with at least 1 DDoS attack / month

10% of organizations believe their connected devices are fully secure

Source: 2016 Telecom.com IoT Outlook

보안 위협 동향



ONLY **20%**

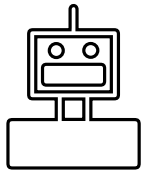
OF IT PROS ARE CONFIDENT USERS AVOID PHISHING

2015 CyberThreat Defense

85,000

MALICIOUS IPS LAUNCHED EVERYDAY

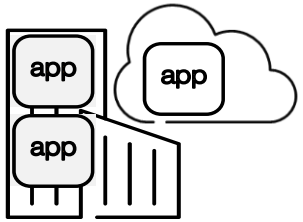
Threat Brief Report, Webroot, May 2015



1.1M

BOTS ACTIVELY ATTACKING

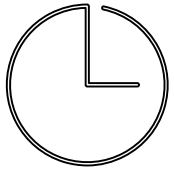
Symantec Internet Security Report 2016



36%

NO CYBER-ATTACK RESPONSE IN PLACE

F5 Networks Survey Research 2016

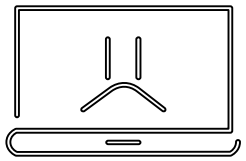


EVERY

23 min

A WEBSITE IS HIT BY A CRITICAL EXPLOIT

(F5 Research)



86%

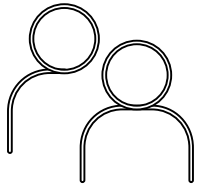
OF WEBSITES HAVE AT LEAST 1 SERIOUS VULNERABILITY

WhiteHat Security Statistics Report 2015

56

AVERAGE NUMBER OF VULNERABILITIES PER WEBSITE

WhiteHat Security Statistics Report 2015

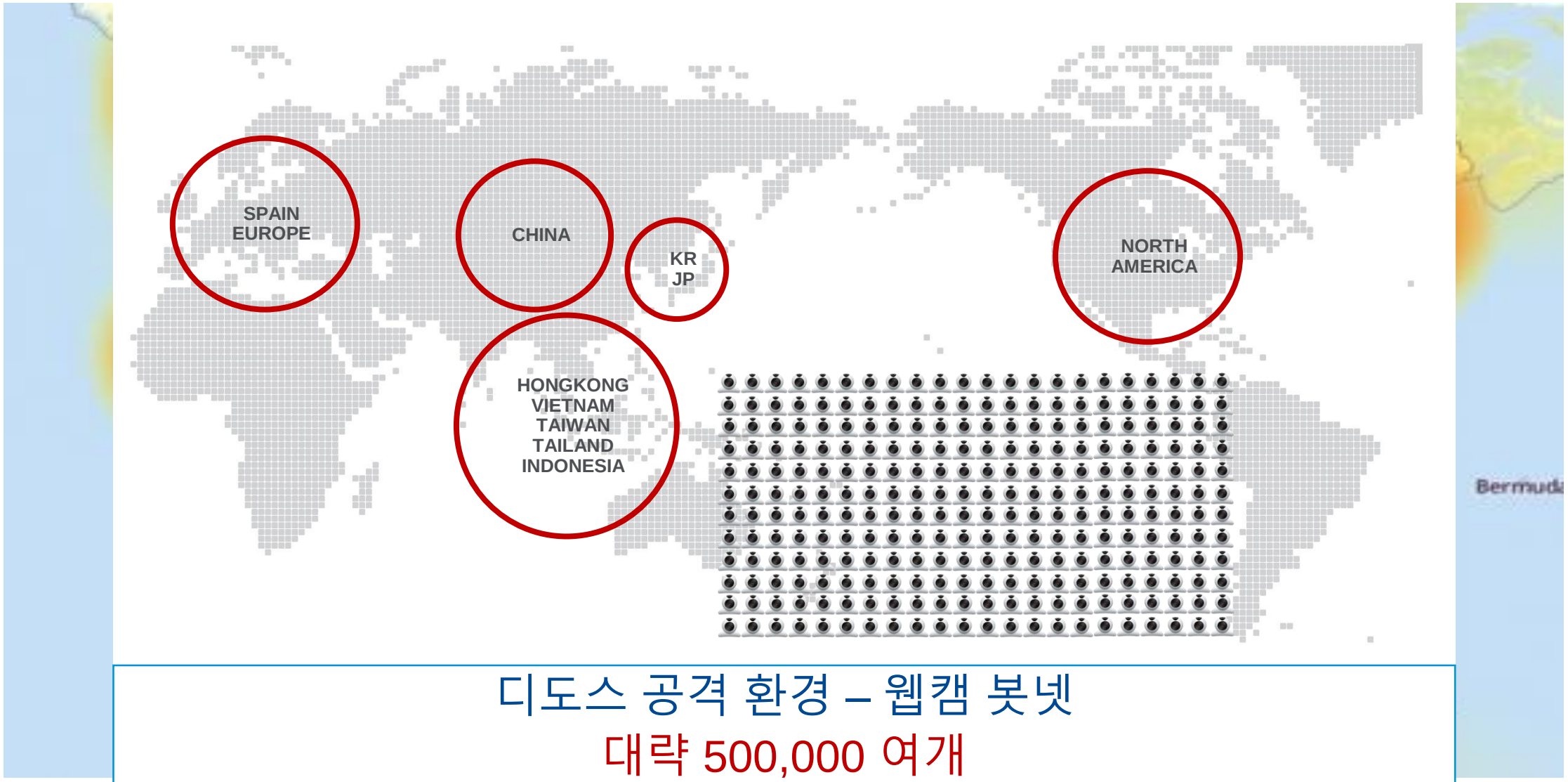


80%

OF IT PROS: THREAT INTELLIGENCE HELPS PREVENT ATTACKS

2015 Importance of Cyber Intelligence, Ponemon Institute

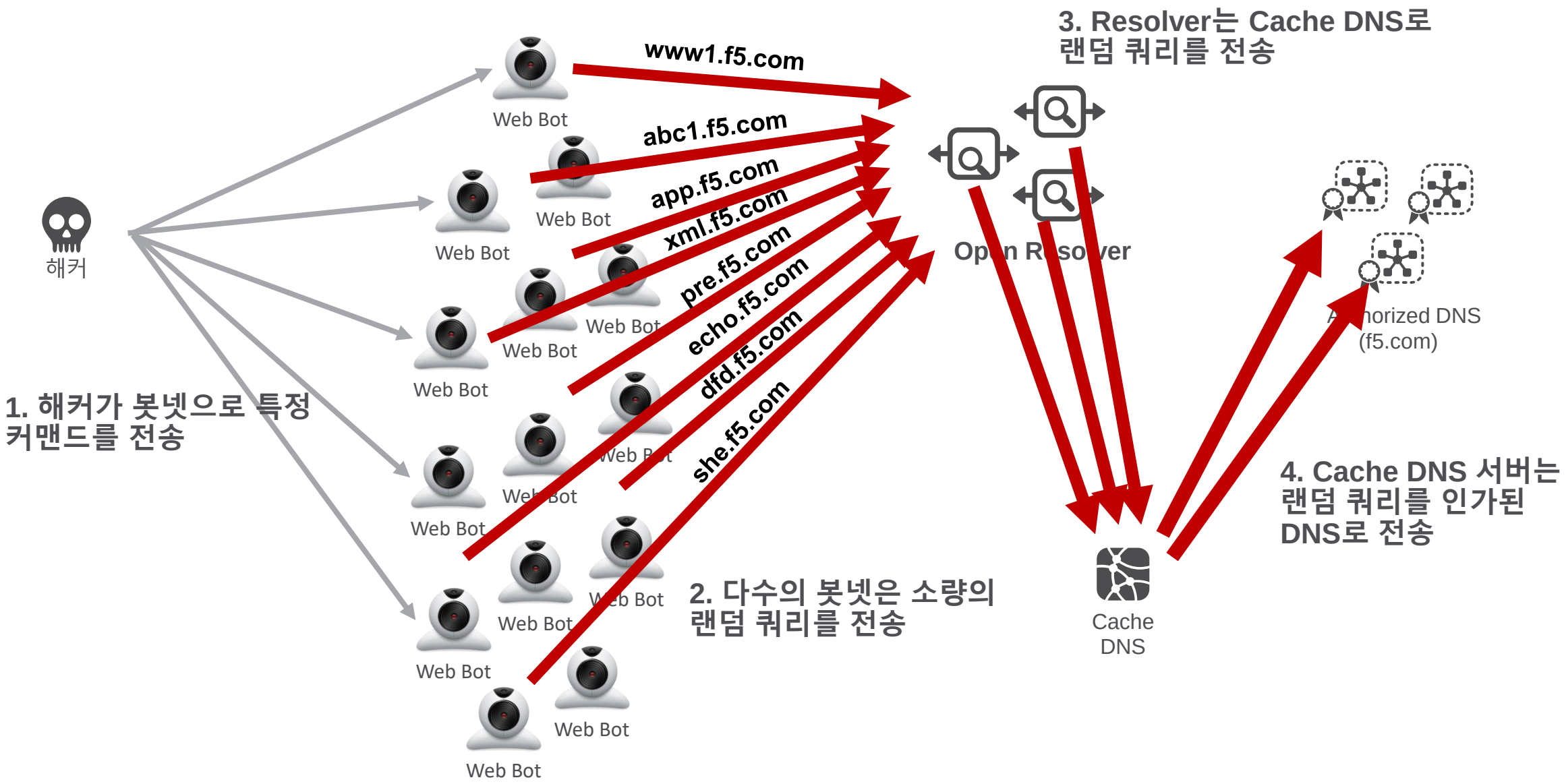
Mirai 봇넷의 전세계 분포도



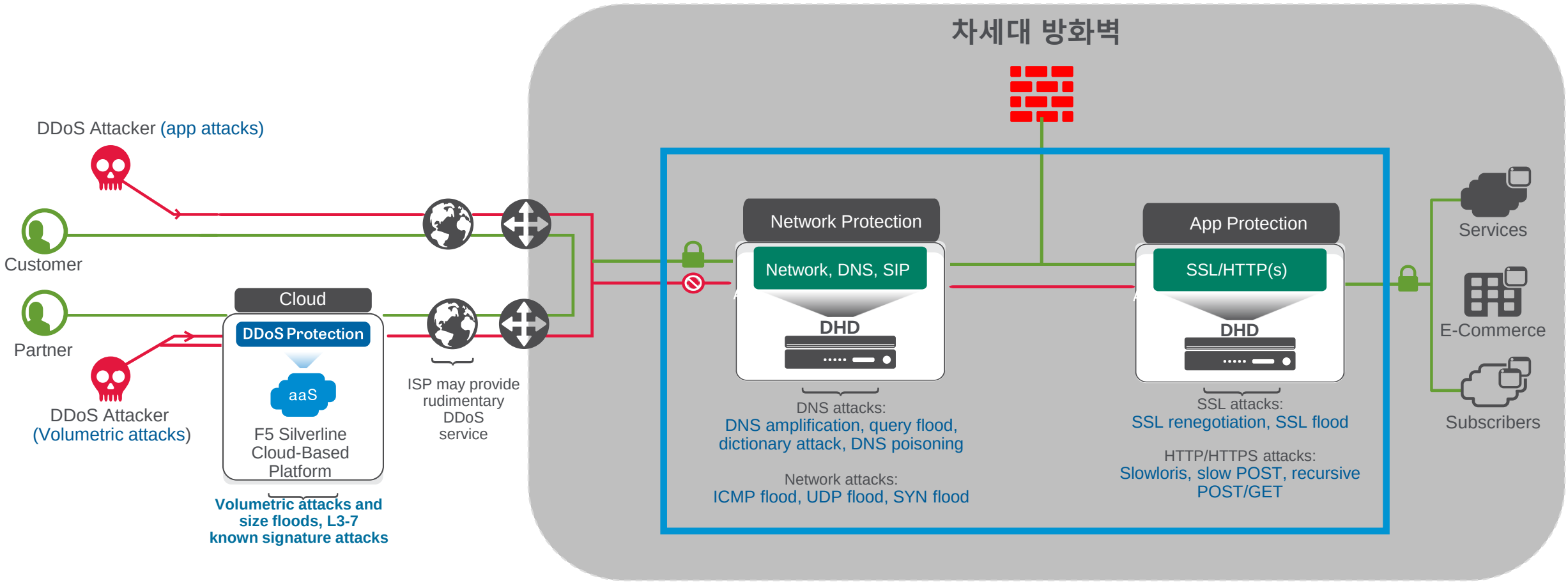
디도스 공격 환경 – 웹캠 봇넷

대략 500,000 여개

IoT 봇넷 (예제) – DNS Water Torture Attack



IoT 봇넷 DDoS 공격 대응을 위한 하이브리드 구성 방안



하이브리드 | **대규모 형태의 디도스 공격에 대해서 온프렘 DDoS 제품이 Silverline로 신호 전송 후 탐지 대응**

1

증가하는
채널의 다양성

2

이커머스와
연계

3

금융서비스
(빈도와 주기)의
양자 도약

모든 온라인 서비스와 지불수단의 통합으로 발전

+

+

+

금융 서비스는 여전히 복잡한 xCommerce의 복잡한 밸류 체인속에서 그 적합성을 찾고 있습니다.

Source : F5 Sponsored Industry Survey

보안과 서비스 속도의 불안은 지속적인 쇼핑의 저해 요인

문의: 온라인 쇼핑을 저해하는 주요 요인은 무엇인가?

	 Australia	 New Zealand	 China	 Hong Kong	 India	 Indonesia	 Malaysia	 Philippines	 South Korea	 Taiwan	 Thailand	 Singapore	 Vietnam
개인 프라이버시 및 보안의 불안	MEDIUM	MEDIUM	HIGH	HIGH	HIGH	LOW	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	LOW
서비스 응답속도 지연	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	LOW	LOW	LOW	HIGH	MEDIUM	LOW	MEDIUM	MEDIUM

High >25% of respondents; Medium >15-25% of respondents; Low <15% of respondents

Source : F5 Sponsored Industry Survey

최근 보안 위협의 타겟이 되는 금융권

84% 의 금융회사는 사이버 위협을 최우선 과제로 선정 DTTC Survey, Dark reading

59% 의 피싱사기는 주로 FSI(금융권)의 지불 서비스 대상 awpg.org Q3 2014

27M 사용자가 금융 맬웨어로 22.9M건의 공격으로 피해

Kaspersky labs

3.24 더 많은 금융 맬웨어 공격은 안드로이드를 겨냥하였고 2014년에는 2,317,194건에 달함 Kapersky labs

360M 계정에서의 세일즈 기밀정보 유출 Bank tech

금융 맬웨어인 Neverquest는 **15,000** 이상의 컴퓨터 봇넷을 보유한 ‘Vawtrak’로 다시 출현 source

맬웨어 위협 트렌드 – 증가 & 대상

25% 실제로 백신 소프트웨어의 맬웨어 탐지율

50% 보안장비들을 우회 하기로 설계된 맬웨어 코드 비율

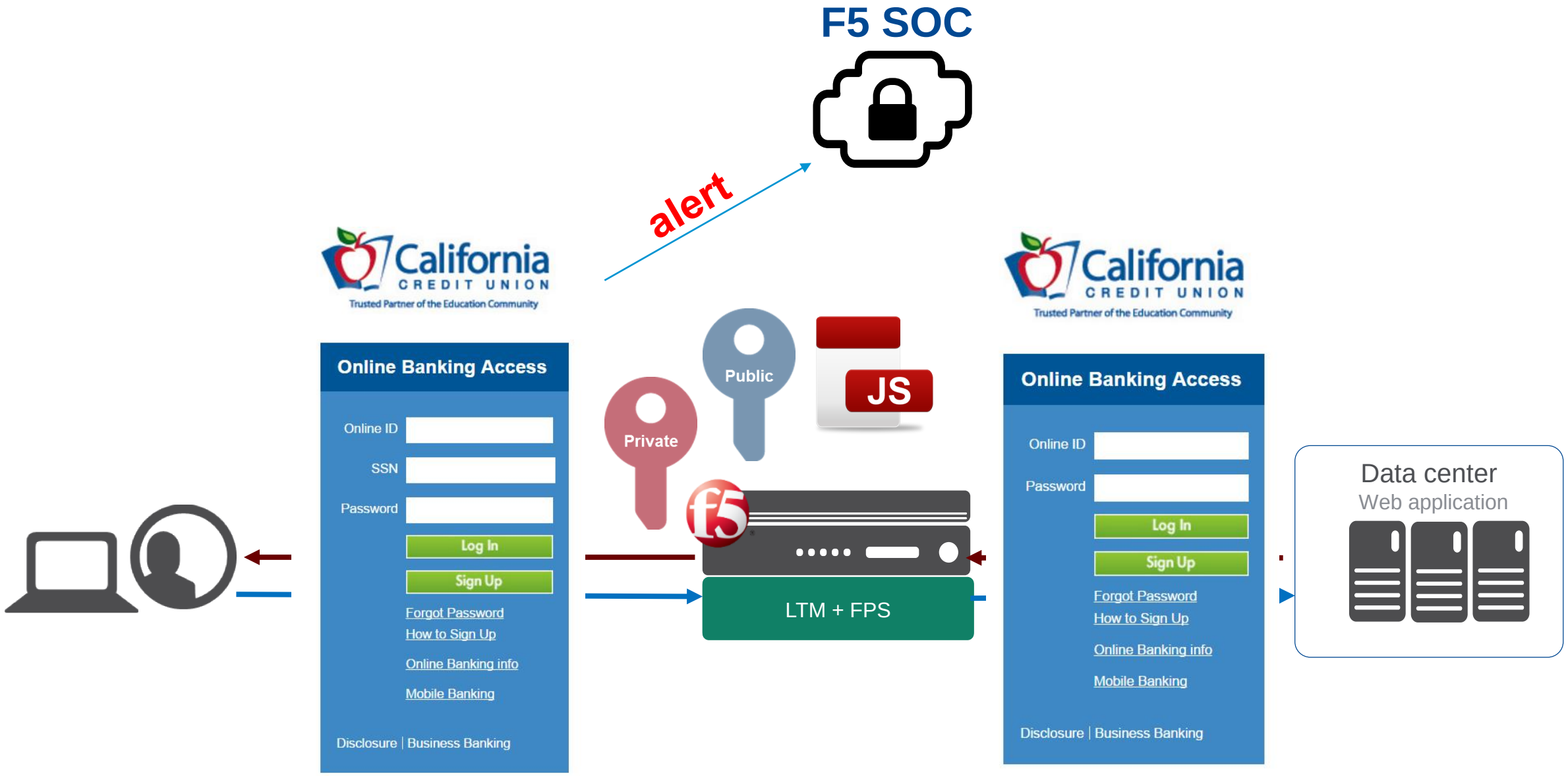
79% 현재의 맬웨어 변형이 대부분 Trojans일 가능성

82% 고객들로 부터 금융사기사건을 배운 기업들의 비율

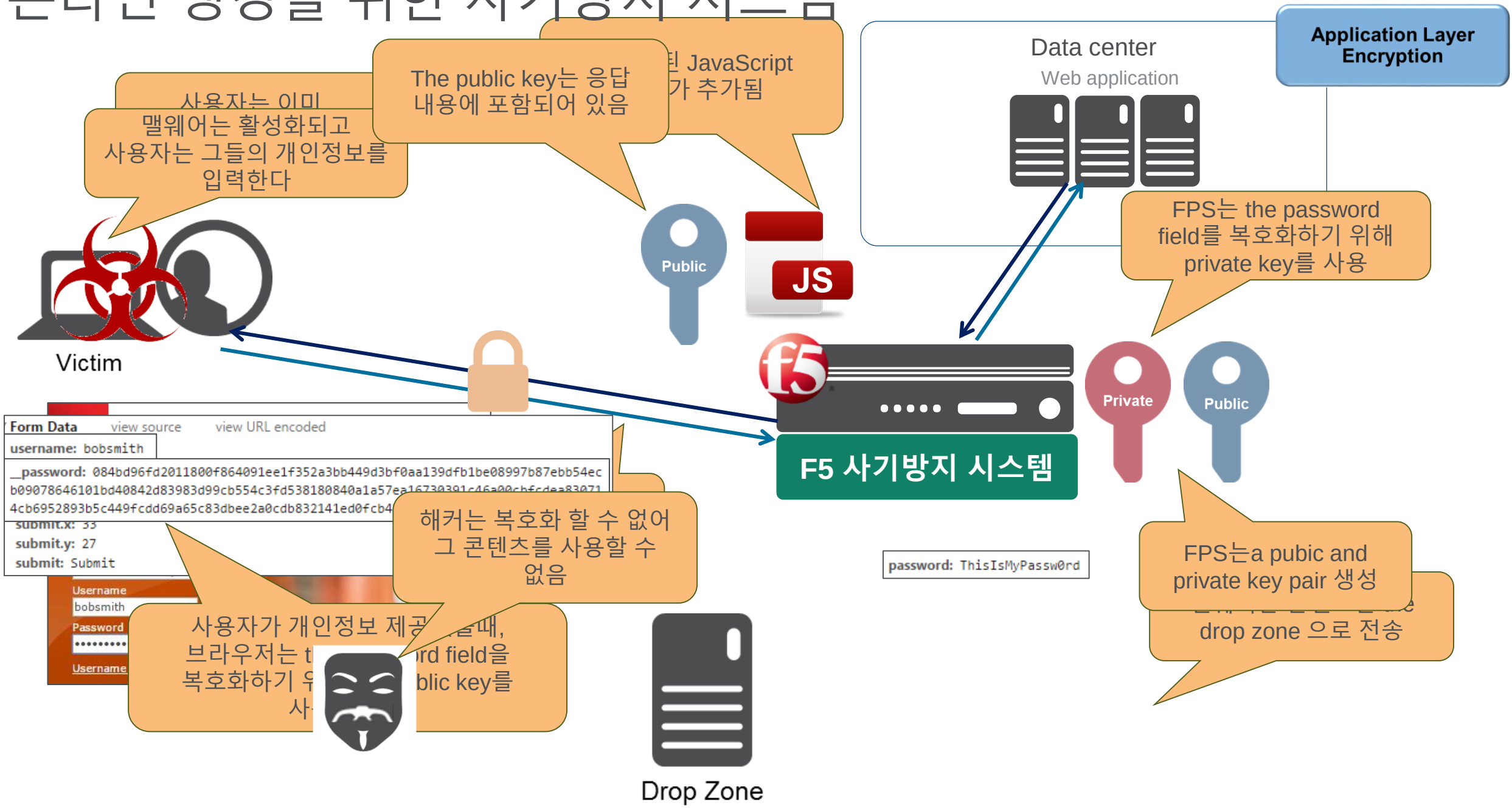
Data sources: Dark Reading, PandaLabs, and ISMG

온라인 금융거래의 안전한 서비스를 말하다

온라인 뱅킹을 위한 사기방지 시스템



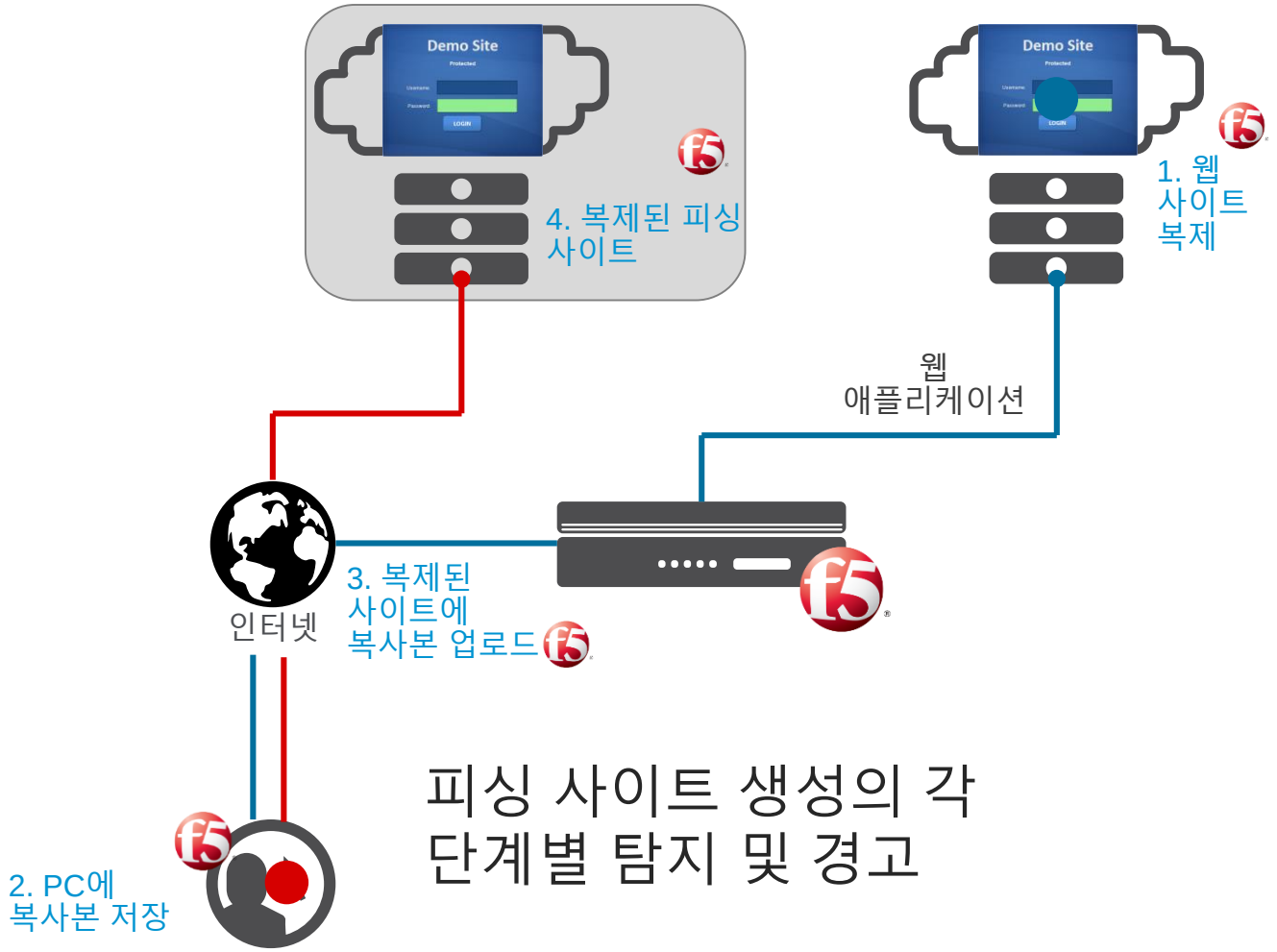
온라인 뱅킹을 위한 사기방지 시스템



최신 피싱 공격에 대한 탐지 및 방지

고급 피싱 위협을 조기에 식별하여 그 공격을 방지

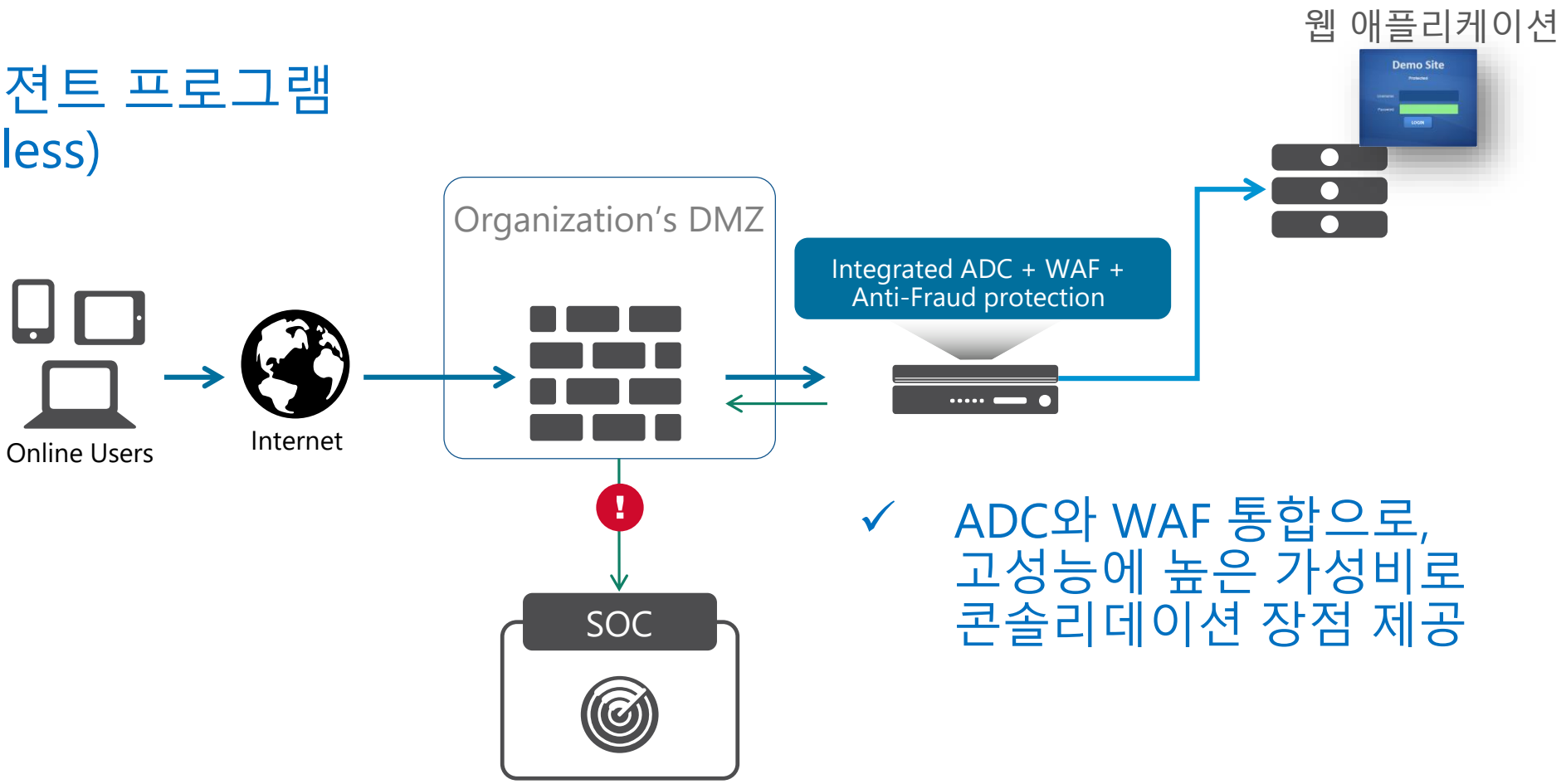
- 다른 서버로의 사이트 복제에 대한 알람 기능 제공
- 로그인 및 피싱 사이트에 대한 시도가 있을 경우 알람
- 감염된 서버에 대한 즉각적인 셧다운
- 피싱 침해가 된 사용자에 대한 접근 로그 제공



피싱 사이트 생성의 각 단계별 탐지 및 경고

사기방지 시스템 구축시 기대효과

✓ 별도의 에이전트 프로그램 없음 (Agentless)



✓ ADC와 WAF 통합으로, 고성능에 높은 가성비로 콘솔리데이션 장점 제공

✓ 통찰력과 가시성을 제공할 수 있는 실시간 사기 탐지 경고를 위한 알람 제공

1

증가하는
채널의 다양성

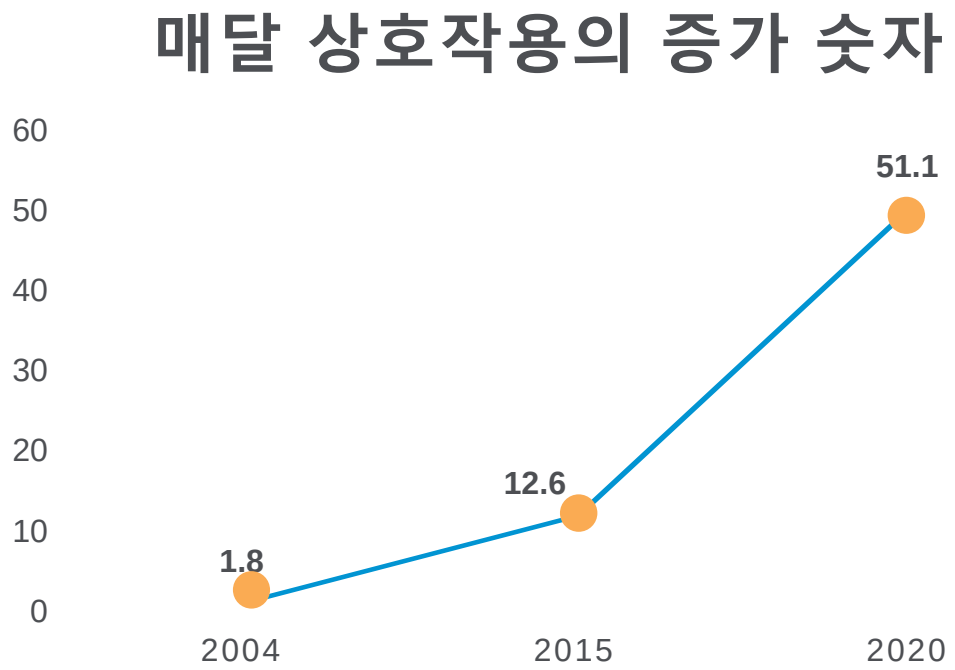
2

이커머스와
연계

3

금융 서비스
(빈도와 주기)의
양자 도약

금융 서비스의 혁신적인 도약:
더욱 빈번해지는, 의미있는 상호작용

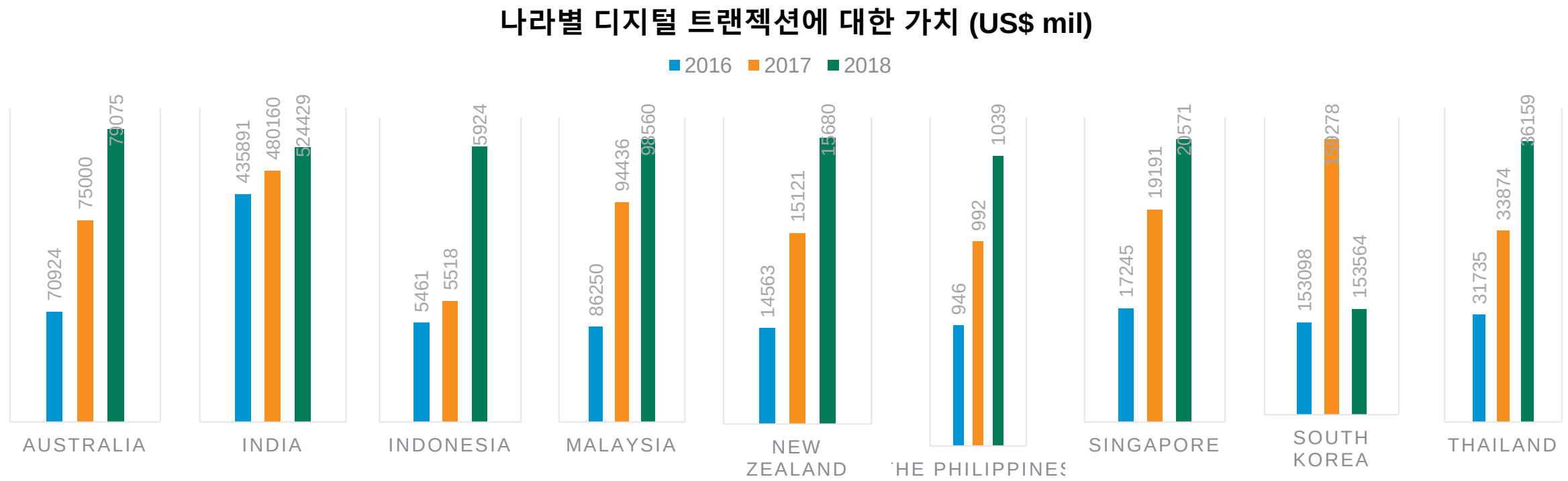


2020년 까지:

은행들이 적극적인 홍보활동을
늘리면서 (교차 세일, 추가 세일, 자문)
더욱더 많은 자문, 촉진과 집계
서비스, 상호작용의 빈도와 주기는
확대될 것이다.

Source : F5 Sponsored Industry Survey

APAC 고객들은 온라인 쇼핑 분야에 있어서 세계를 주도할 것으로 기대



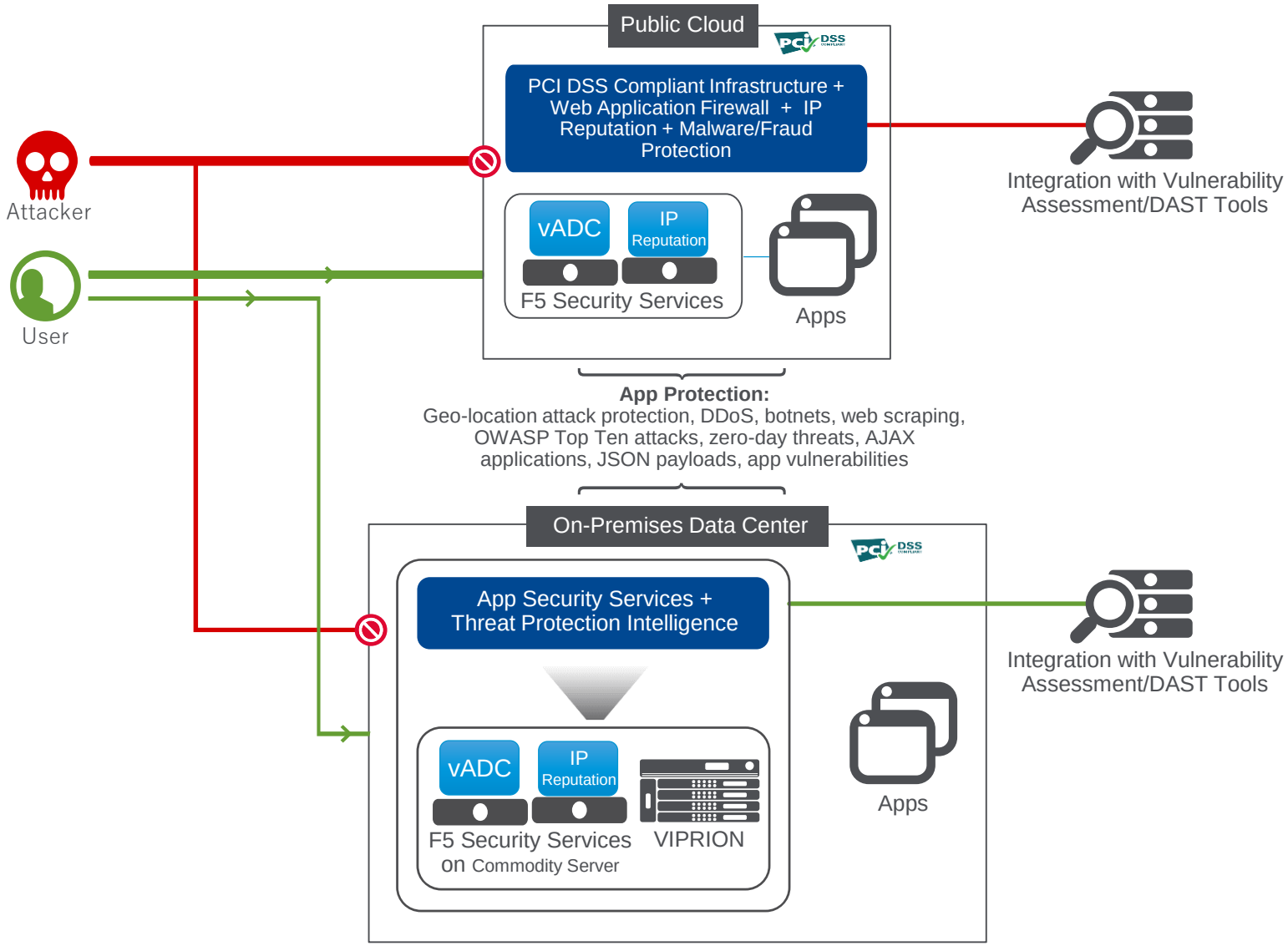
+5.8% +10.8% +10.2% +13.9% +3.9% +6.5% +10.8% +4.9% +12.5%

IDC Analyze the Future

퍼블릭 클라우드 전환에 따른 보안을 말하다

"우리는 퍼블릭 클라우드로 전환은 결정했지만, 데이타센터와 동일한 보안수준을 통한 가용성을 요구하게 된다."

하이브리드 클라우드 기반의 대응 체계

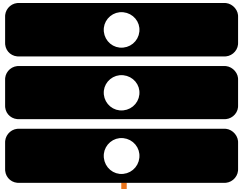


금융 서비스 보호를 위한 기대효과

피싱 공격 방어

단일 제품으로 사기탐지
및 보호를 동시에 제공

신속한 구축 시간



컴플라이언스 준수 보장

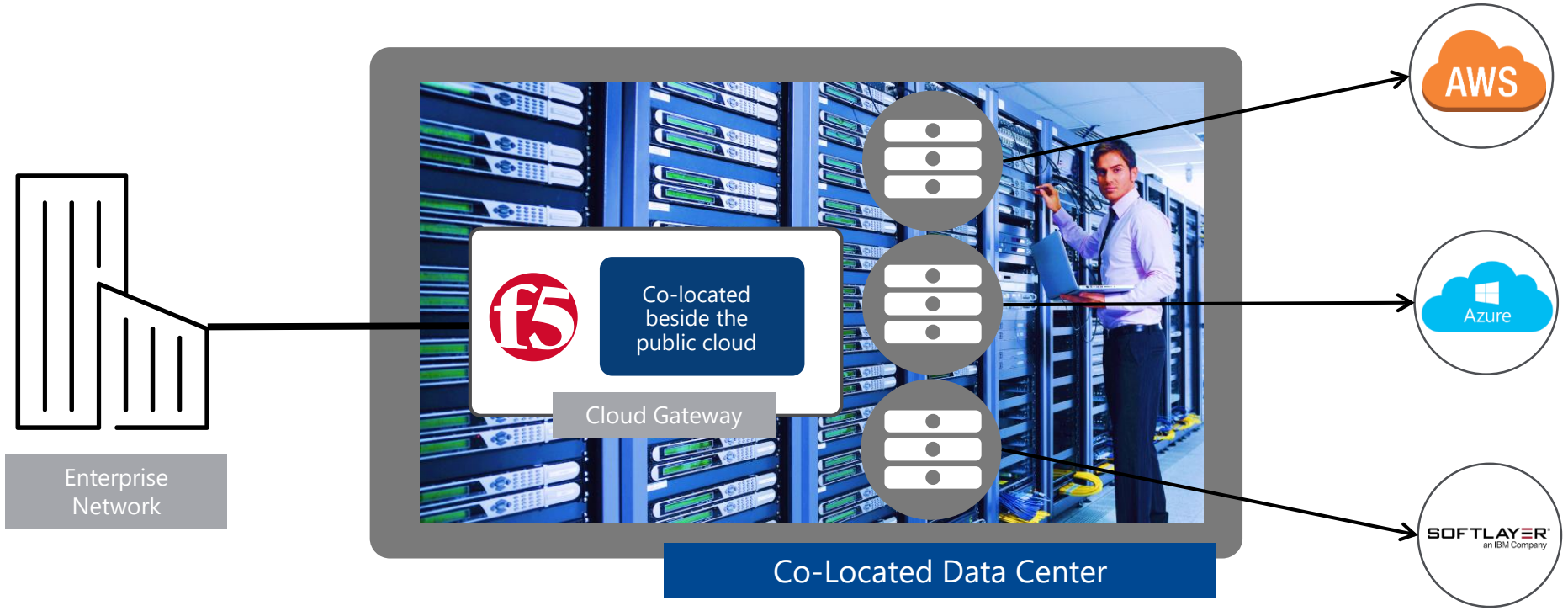
가로챈 정보를
무효화 시킴

즉각적인
사기손실 절감

모든 고객의 디바이스 보호

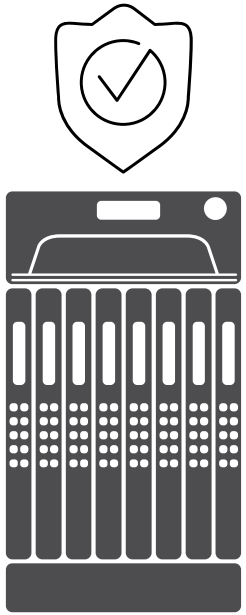
최상의 클래스 지원 및 프로페셔널 서비스

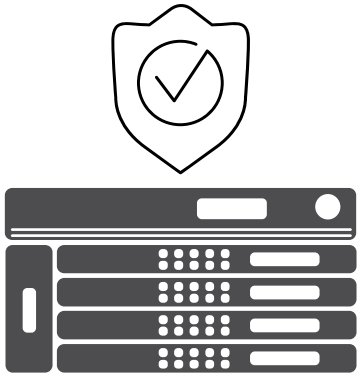
신규 퍼블릭 클라우드의 지속적인 고가용성 유지



기존 데이타센타의 인프라를 퍼블릭 클라우드로
전환시에도 동일 가용성 및 안전한 데이타 관리

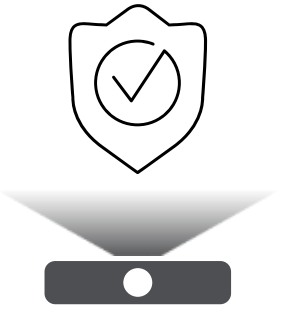
웹방화벽 및 DDoS 방어를 위한 다양한 플랫폼 제공



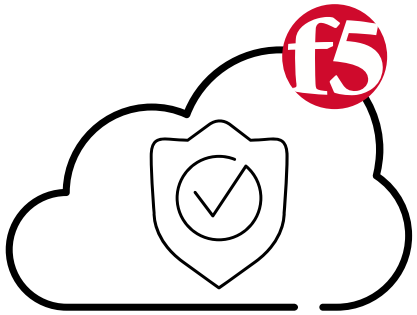


Chassis / Blade Platform

Appliance Platform

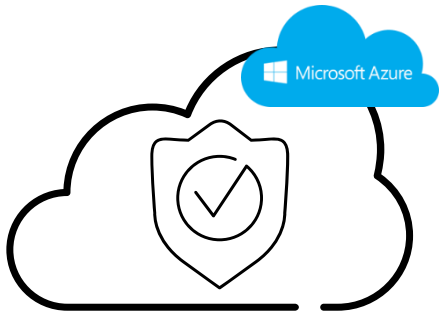


Virtual Appliance

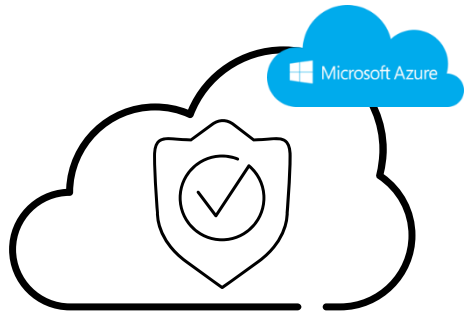


Cloud-based WAF
(WAFaaS)

WAF in AWS
(BYOL, Utility)



WAF in Azure
(BYOL)



WAF Solution for Azure Security Center

SOLUTIONS FOR AN APPLICATION WORLD