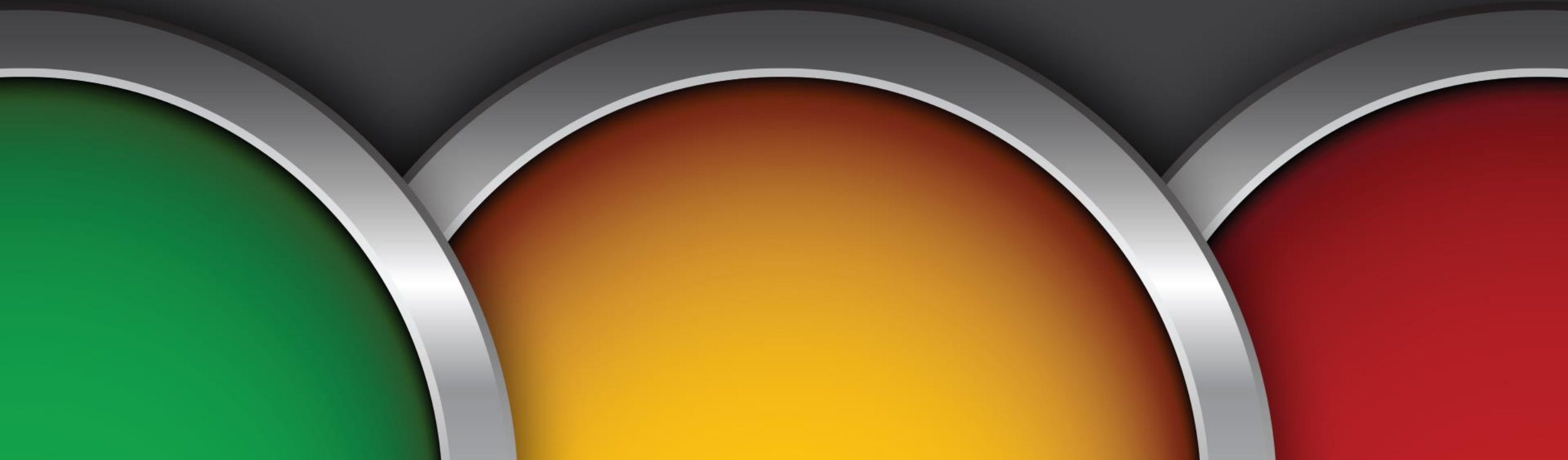
radware
Every second counts

300기가급 복합공격 방어기술과 전략

라드웨어 임흥순 차장

April 10, 2015

Change of cyber attack



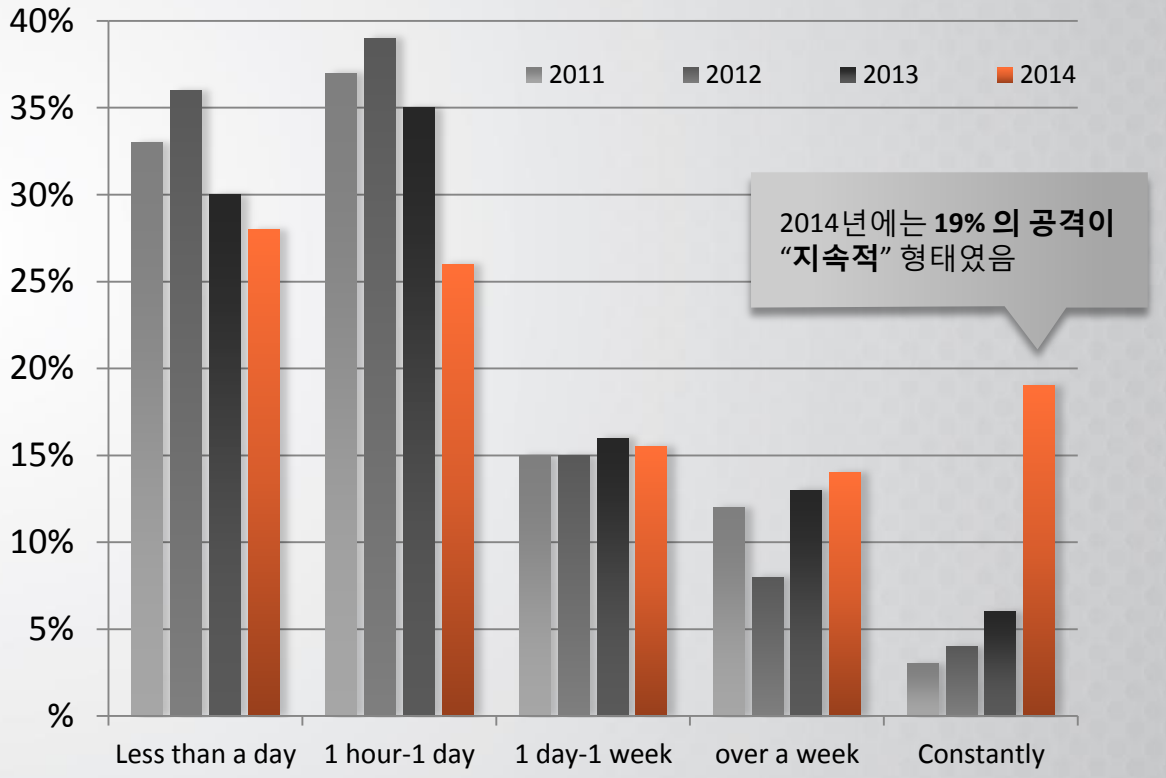
리서치, 통계 분석을 통한 보고서

연간 매출 규모 300억 ~ 10조원의 글로벌 기업을 대상으로…

지속적인 공격의 증가

장기화 되는 공격

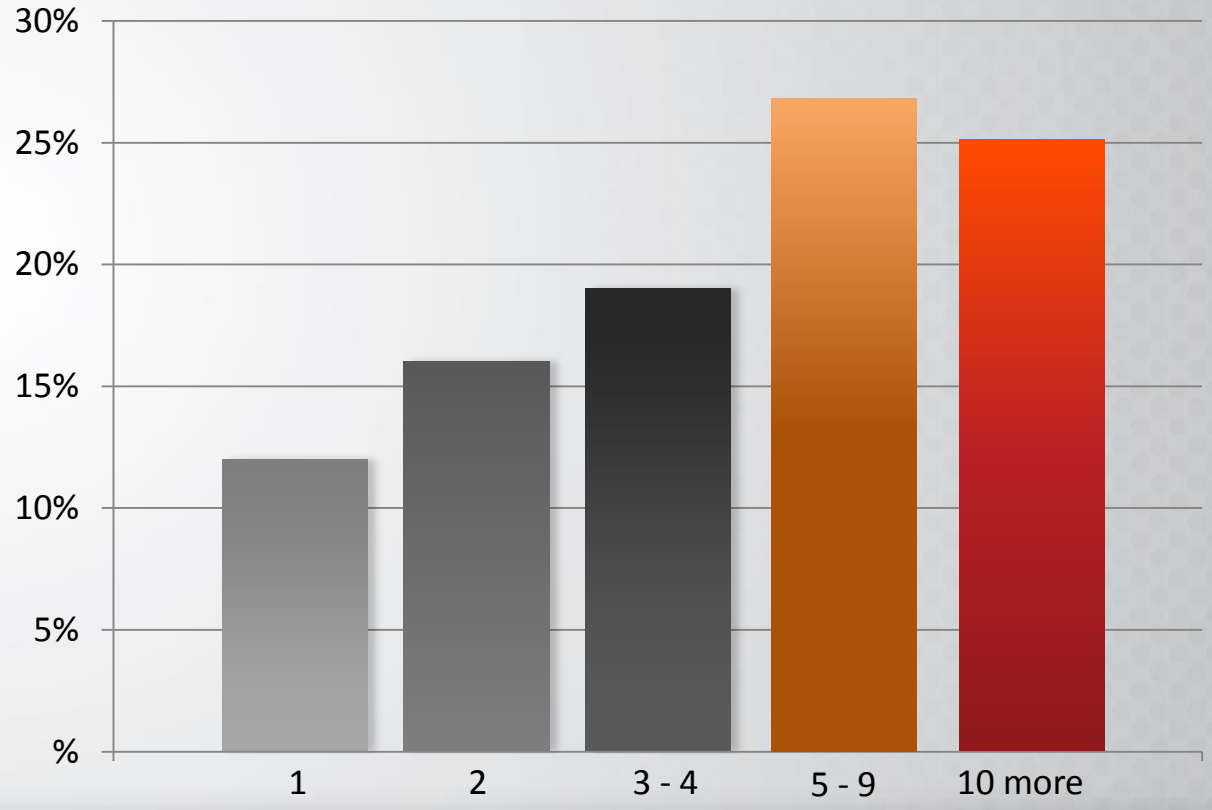
- 2013년 조사 결과에서는 “지속적” 공격이 6%를 초과하지 않았음
- 2014년- 19% 의 공격이 “지속적” 형태
- 52%의 고객은 단지 하루 또는 그 이하의 공격활동에 대응 할 수 있었음



정교한 복합 공격의 증가

멀티 벡터의 정교한 공격

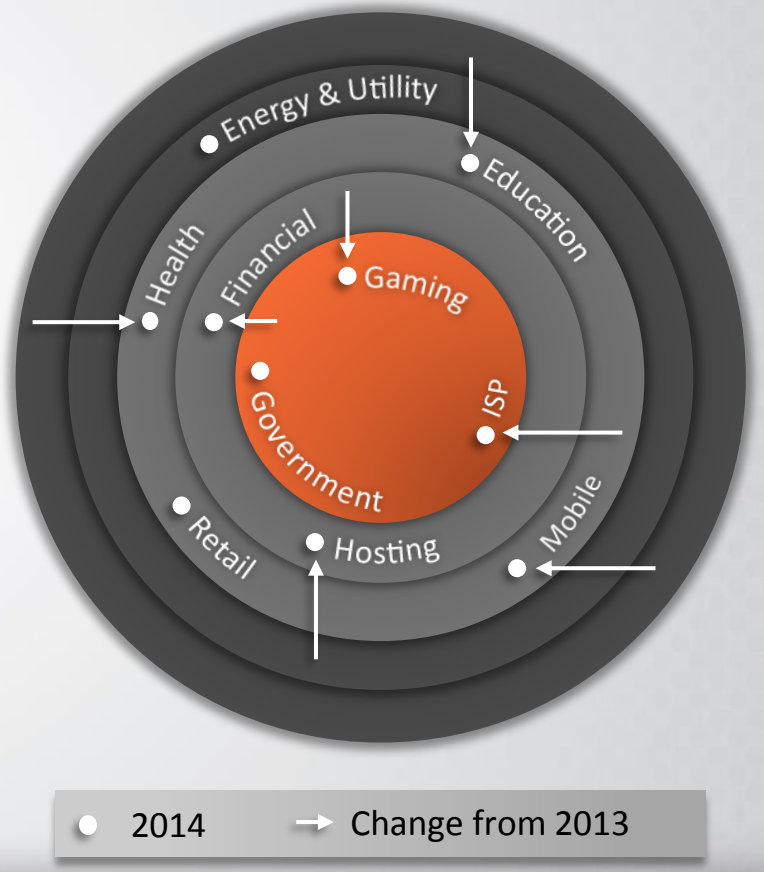
- 50% 이상이 5개 이상의 공격 벡터를 경험
- 순차적 공격으로 멀티벡터를 활용
- Encryption 을 포함한 애플리케이션과 네트워크 벡터가 혼합된 정교한 공격의 증가



어느 누구도 면역력 없고, 타겟도 예상하기 어려움

다양한 산업군으로 확장되는 공격

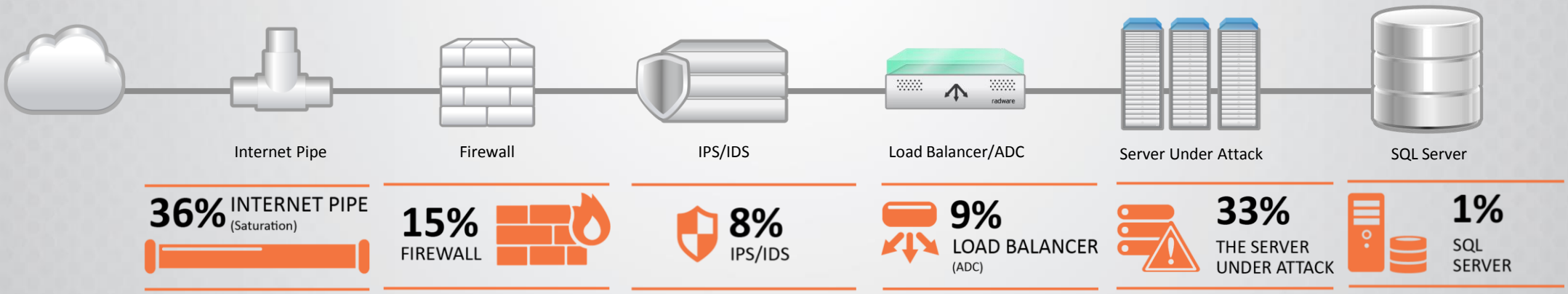
- **의료 및 교육 분야** – 예상치 못했던 대상으로 최근 높은 리스크를 가진 업계로 급 부상중
- **게임사, 호스팅 및 ISP** – 공격 노출 증가 상태임
- **금융 서비스 분야** – 이미 공격에 노출되어 어느 정도의 리스크는 제거된 상태



인터넷 파이프 – 2014 No.1 중단 포인트

최초로 인터넷 파이프가 디도스 공격의 대표 병목 구간으로 자리잡음

디도스 공격 유입시 네트워크 구간의 서비스들과 구성 요소는 병목 현상을 유발



대용량 복합공격 - 글로벌 사례

2012. 9

2013. 3

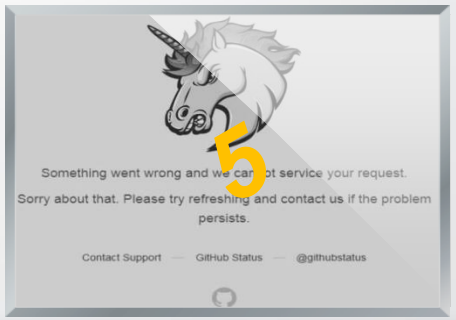
2013. 5

2013. 5

Duration, Volume, Complexity

2014. 6

2015. 1



2015. 3

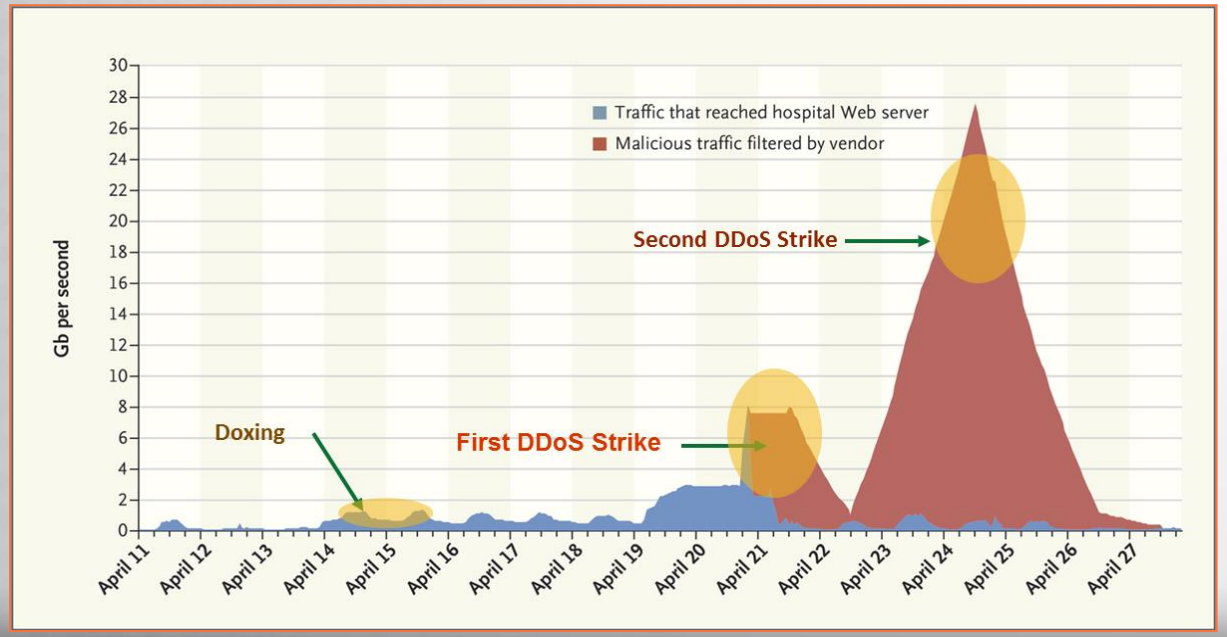
2015. 4

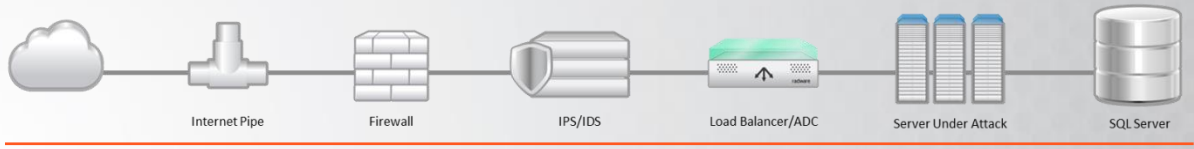
대용량, 복합 공격의 표본 - 공격사례

15개의 다른 공격 벡터 사용

웹 공격과 DDoS 혼합의 대용량 공격

한달 이상 지속적인 공격

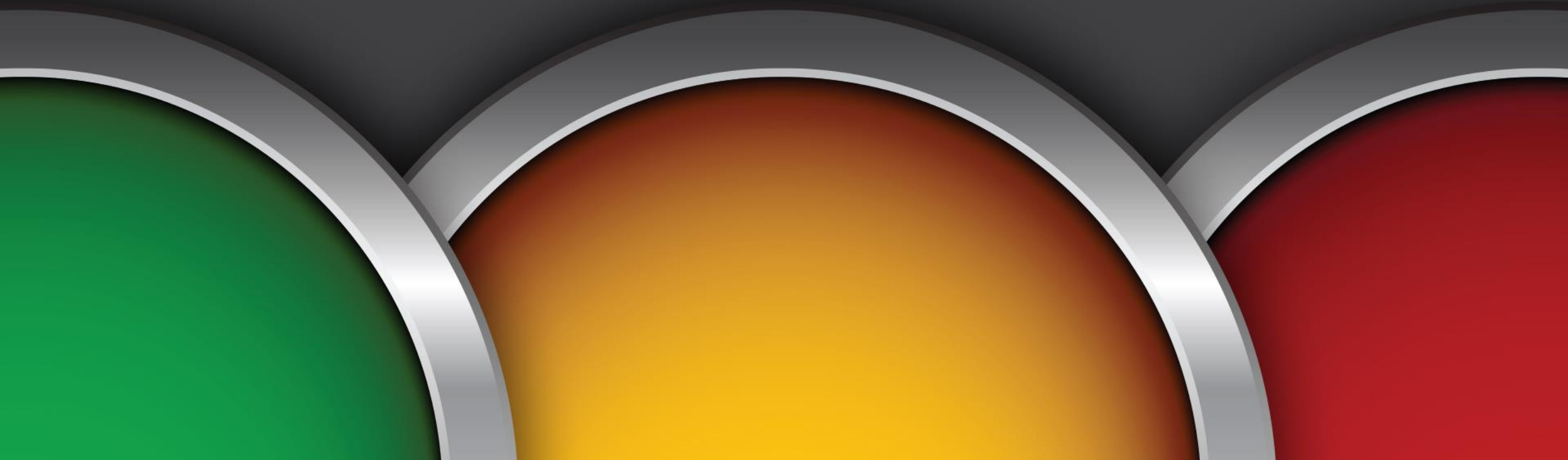




Infra	State	Application
UDP Fragmented Flood	TCP Out Of State Flood	Slowloris
DNS Reflection	UDP Scan	SQL-Injection
UDP Flood (PPS)	Zero Payload attacks	XSS
	Zero sequence number attacks	Worm infection - Mydoom
	Invalid ACK number attacks	SIPVicious - Scanning tool
	ICMP Flood	Web-etc/passwd-Dir-Traversal

radware
Every second counts

Why Should You Care?



서비스 수준이 비즈니스에 미치는 영향

네트워크 중단의 총 피해

52% of companies report:

total damage of network outages and performance degradation:

More than **6억원**

Per Hour

(based on 547 US & EU companies)

중단으로 인한 생산성 손실

End-user **Productivity losses** from outages has

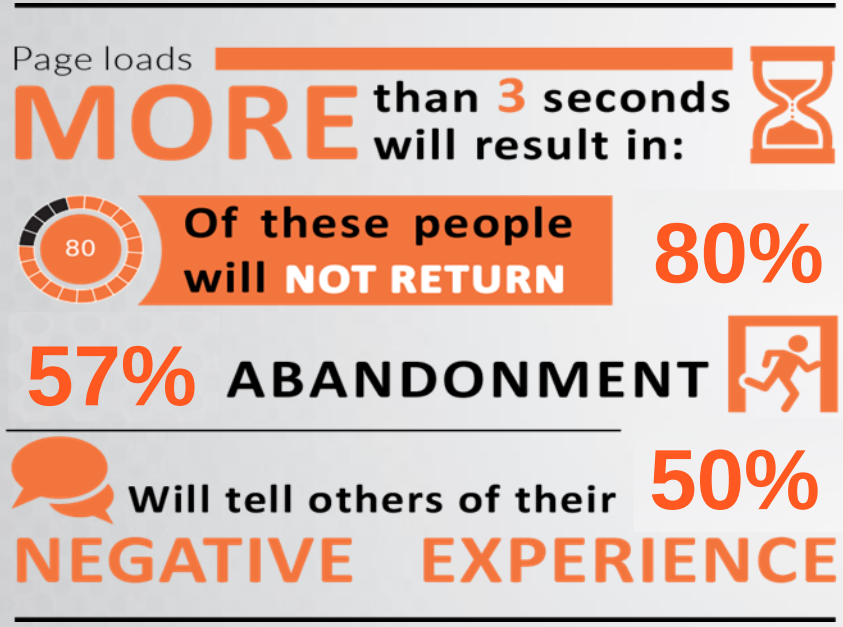
INCREASED

46%

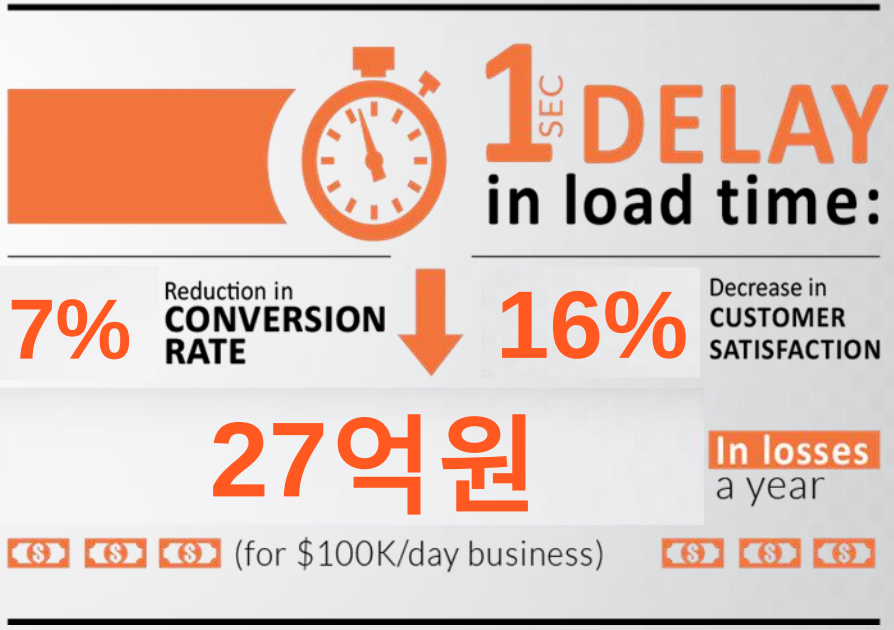
Today more than ever, TIME IS MONEY

서비스 수준이 비즈니스에 미치는 영향

포기와 부정적인 평판



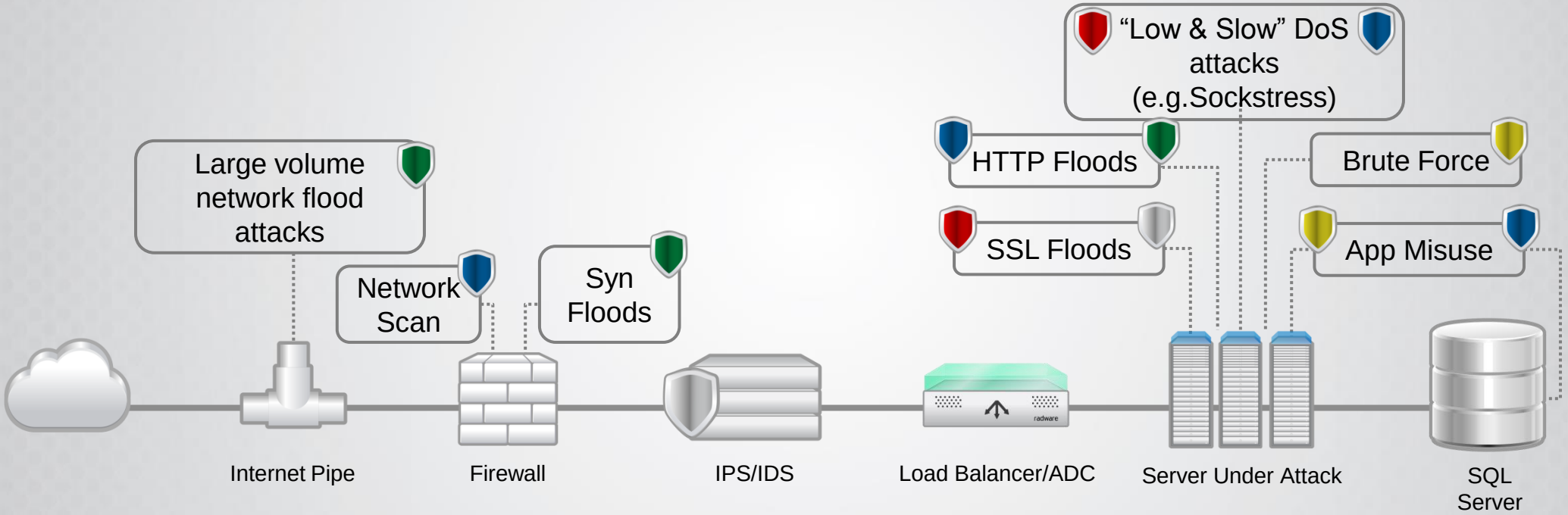
낮은 구매율과 만족도 하락



radware
Every second counts

How do we do it?

통합 하이브리드 솔루션의 필요

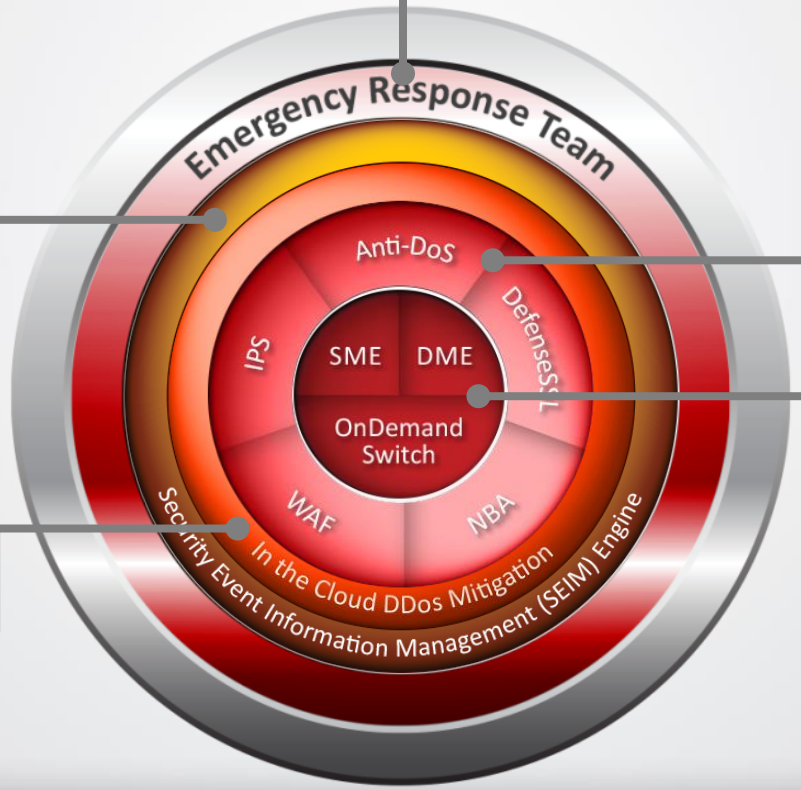


통합 하이브리드 솔루션의 요소

Emergency Response Team support

Integration Monitoring
Integration Management

Multi vector attack mitigation



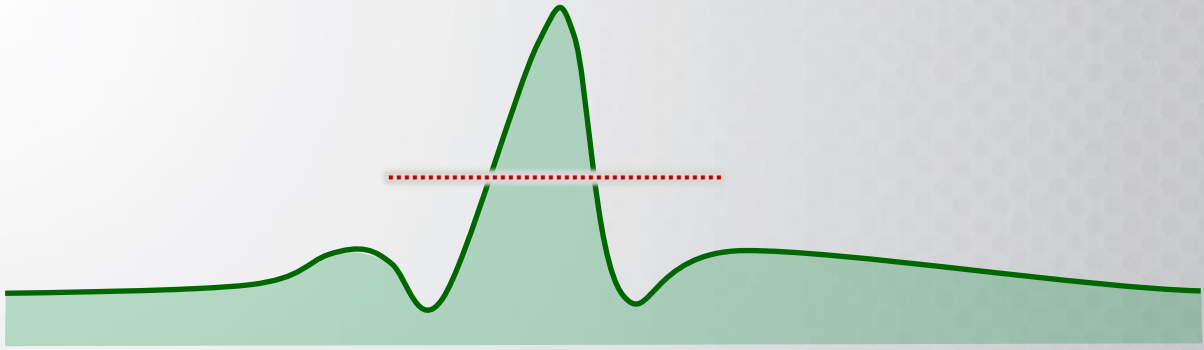
Large volume attack
Cloud Scrubbing Center

Dedicated hardware
Attack & Legitimate

Fuzzy logic을 이용한 행동 기반 분석

행동기반 분석

피상적인 임계치 기반의 분석보다



정상 트래픽의 서비스 레벨에 미치는 영향을 제거하기 위해

지능적인 공격 도구의 무력화 전략

```
HTTP/1.0 302 Found
P3P: CP=NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM
Location: /
Set-Cookie: aaaaaaa=ec95877faaaaaaa_ec95877f; Path=/
```

302 Challenge

```
HTTP/1.0 200 OK
Expires: Sat, 6 May 1995 12:00:00 GMT
P3P: CP=NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 144
Connection: Close

<html><body><script>document.cookie='aaaaaaa=d35baf4eaaaaaaaa_d35baf4e;
path=/';window.location.href=window.location.href;</script></body></html>
```

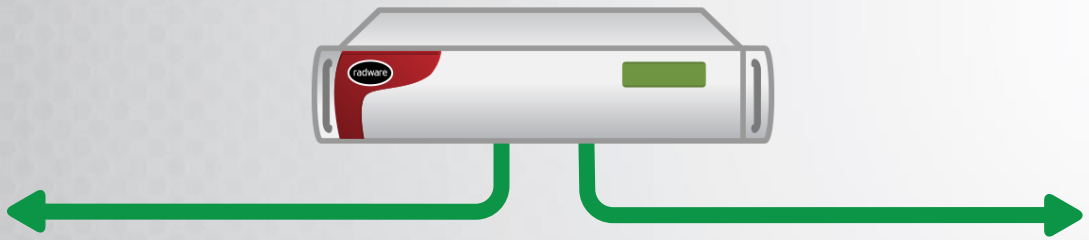
JavaScript Challenge

```
<html><body><script>var $c='a';$0='4';$f='a';$w='4';$L='a';$x='a';$Q='a';$7='a';$T='a';
d='_';$Y='a';$J='=';$K='4';$i='9';$N='4';$s='2';$9='3';$h='7';$G='1';$v='a';$A='e';
2='0';$V='9';$F='a';$a='a';$W='a';$g='a';$n='4';$z='2';$4='a';$u='a';$b='a';$1='a';
C='a';$6='_';$S='4';$y='2';$X='3';$H='7';$D='1';$p='e';$8='0';$e='9';document.cookie=(!
?$c:"")+(!({})?$0:"")+(!""?$f:"")+(!({})?$w:"")+(!""?$L:"")+(!NaN?$x:"")+(!""?$Q:"")+(!
?$7:"")+(!NaN?$T:"")+(!""?$i:"")+(!""?
N:"")+(!""?$s:"")+(!0?$2:"")
(!""?$V:"")+(!4?$F:"")+(!""?$a:"")+(!0?$W:"")+(![]?$g:"")+(!4?$n:"")+(![]?$z:"")+(!NaN?
4:"")+(!""?$u:"")+(!NaN?$b:"")+(!NaN?$1:"")+(!""?$C:"")+(!0?$6:"")+(!0?$S:"")+(!""?
y:"")+(!NaN?$X:"")+(!NaN?$H:"")+(!""?$D:"")+(!0?$p:"")+(!0?$8:"")+(!NaN?$e:"")+';
path=/';window.location.href=window.location.href;</script></body></html>
```

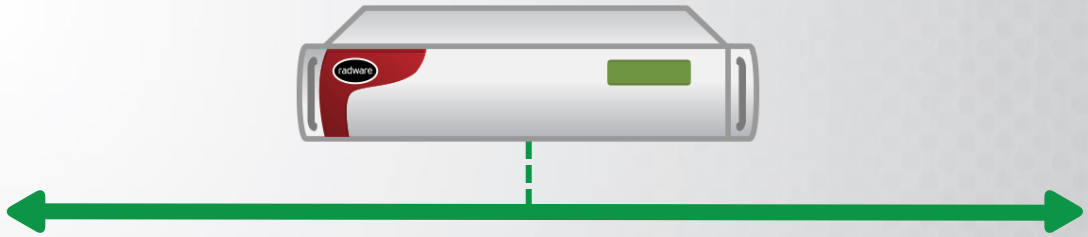
Advanced JavaScript Challenge

유연한 네트워크 구성을 통한 동적 완화

In-Line when you must



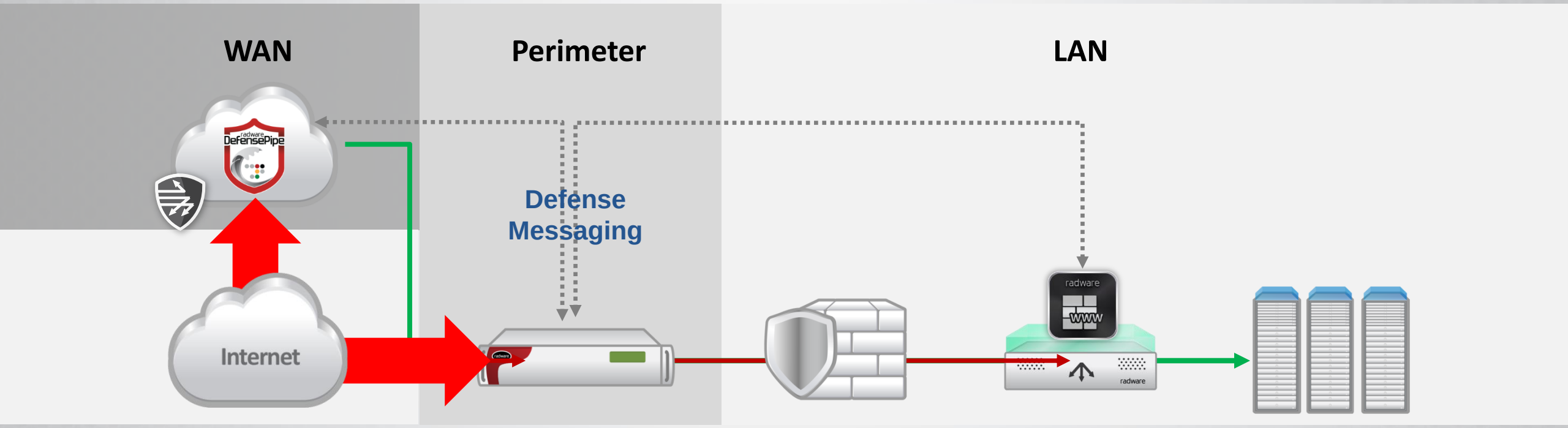
Out-of-Path when you can



서비스의 보안에 미치는 영향을 최소화

협력을 통해 향상되는 보안

분산형 아키텍처는 서비스 수준 저하를 최소화 하고 서비스 중단을 보호

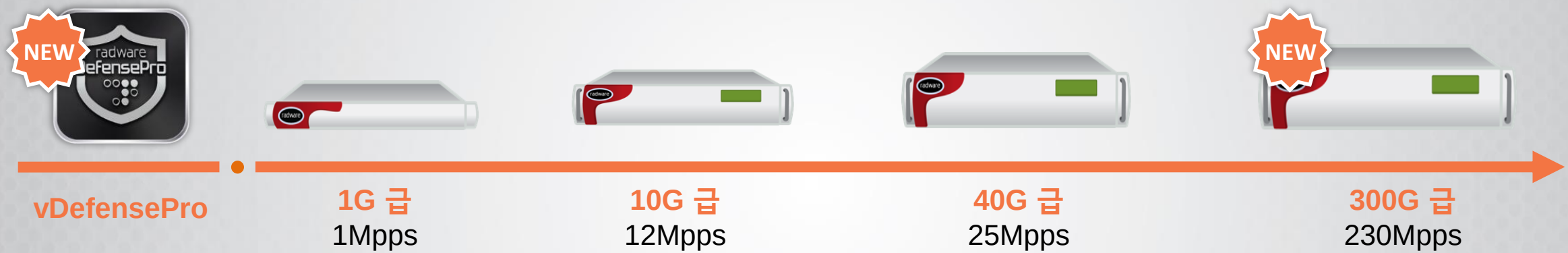


대용량 공격으로부터 인터넷 회선을 보호

광범위한 공격 방어 시스템

radware
Every second counts

테크니컬 하이라이트

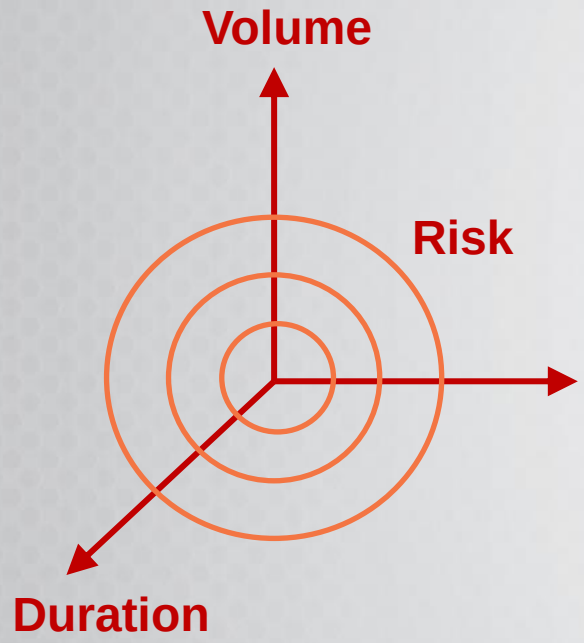


모든 규모의 엔터프라이즈 /
클라우드 데이터센터의 경계

대형 데이터센터 /
캐리어 네트워크의 경계

요약

	Detection	Mitigation
Coverage	✓	✓
Accuracy	**High**	**High**
Time	**Sec**	**Sec**



- Net DDoS
- App DDoS
- Low&Slow
- SSL Attack
- Web Attack

Outage
Slowdown → ↓Revenue ↓Productivity ↓Brand

AMS → System, Service

Cloud Scrubbing ↔ Hybrid Solution

On-Premise

- Anti-DoS
- NBA
- IPS
- Defense-SSL
- WAF

Reporting

ERT 24 / 7

radware

Every second counts