웹(Web)방화벽 솔루션

DeepFinder

2018.01

융합보안사업부

DOUZONE
www.douzoneon.com

Maximizing
Potential

CONTENTS

I. 제품소개

II. 웹방화벽 특장점

III. 도입사례

IV. 고객사

Ⅰ. 제품소개

1. 제품개요
2. 구성도
3. 특징
4. 주요기능

DeepFinder는 온프레미스 환경을 비롯하여 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드 등 다양한 환경에 구축 가능한 클라우드 웹 방화벽으로 성능 및 속도 저하 없이 Full SSL Inspection이 가능합니다. 오토스케일을 지원하고 속도 및 가용성이 우수하여 최근 클라우드 환경으로 이전하는 많은 기업에서 도입하고 있습니다.

보안이슈 대응

SSL 가시성 확보

- 웹 서버가 복호화한 트래픽을 필터링하여 속도 및 성능저하 없이 SSL트래픽 분석

클라우드 웹 보안

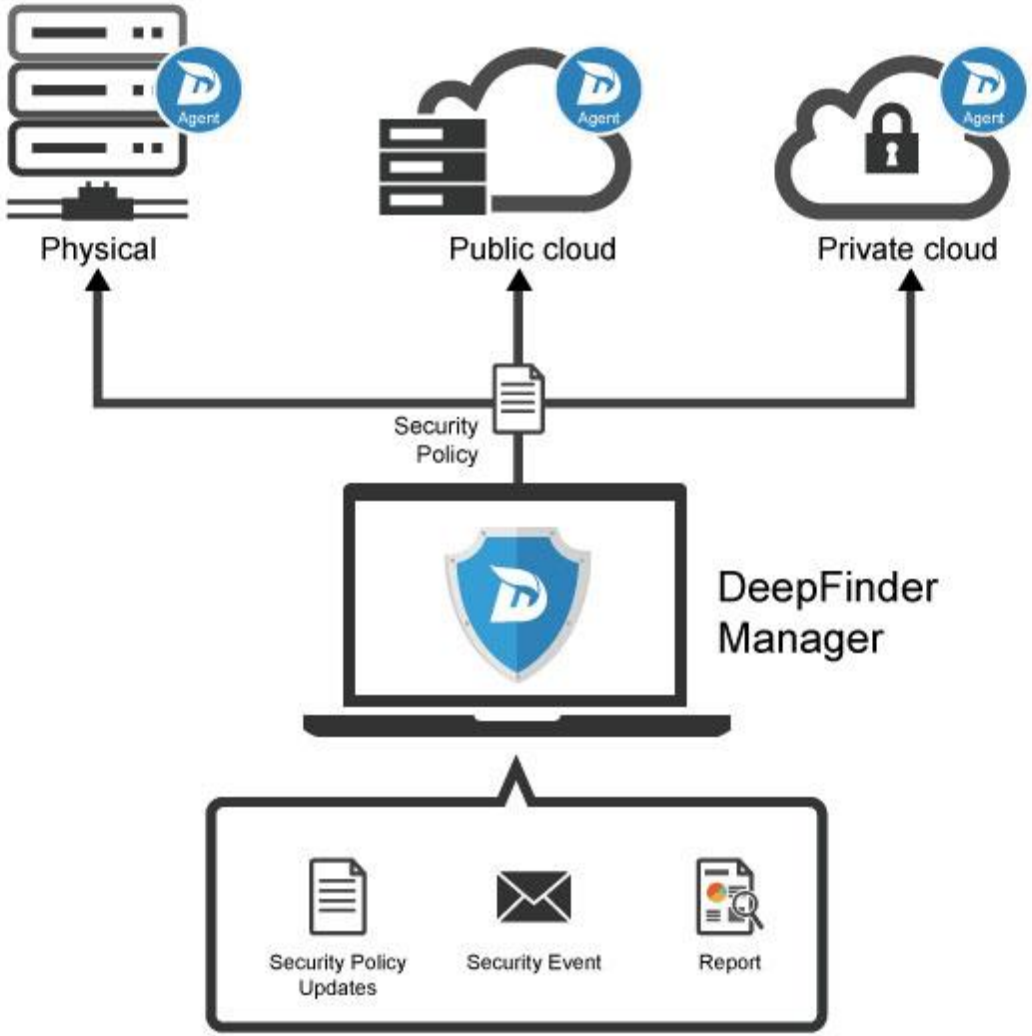
- 다양한 클라우드 환경 지원 (AWS, Azure, Aliyun, Google Cloud Platform, Softlayer, VM, Xen Server 등)
- Auto Scaling 지원(자동 확장/삭제)

개인정보보호법 준수

- 중요정보 유출 방지, 파일 위변조 검사 등
- OWASP Top 10, 국정원 8대 취약점, PCI DSS 6.6 요구사항 대응

2. 구성도

DeepFinder는 웹 서버에 설치되는 Agent와 개별 Agent를 통합관리 할 수 있는 Manager로 구성됩니다. 이러한 논리적인 분산처리 효과 덕분에 설치, 장애, 업데이트 등의 이벤트 발생 시에도 단절없이 보안을 유지할 수 있습니다. 또한 웹 서버의 물리적인 위치나 환경(Legacy 환경 / Cloud Platform 종류/ VM ware, Xen Server, Hyper-V / OS 종류) 에 관계없이 설치 및 통합관리 할 수 있어 보안의 편의성과 연속성을 유지할 수 있습니다.



3. 특징

Cloud 최적화

- 다양한 클라우드 환경 지원 (AWS, Azure, Aliyun, GCP, Softlayer, Xen Server 등)
- Immutable Infra 지원 (Docker, Vagrant, AWS AMI, ECS, BeenStalk, CloudFormation 등)
- Auto Scaling 지원 (솔루션 자동확장/삭제)

서비스 중단없이 보안 구현

- 서비스 무중단 Agnet 설치/수정/삭제
- 기존 네트워크 구성 변경없이 구축 (IDC, IaaS, SaaS, Paas, BPaaS 등)
- 트래픽에 따른 라이선스 갱신 필요 없음
- 이중화 구성(High Availability) 필요 없음

편리한 운영관리

- 전세계 웹 서버의 물리적 위치, 네트워크 구성, 클라우드 환경에 관계없이 통합관리
- 웹 기반 매니저 콘솔(Drag&Drop)로 누구나 보안 설정 가능
- Multi-tenancy 환경에서 tenant 별로 계정 관리
- 계정별 리포트 자동 생성 및 발송

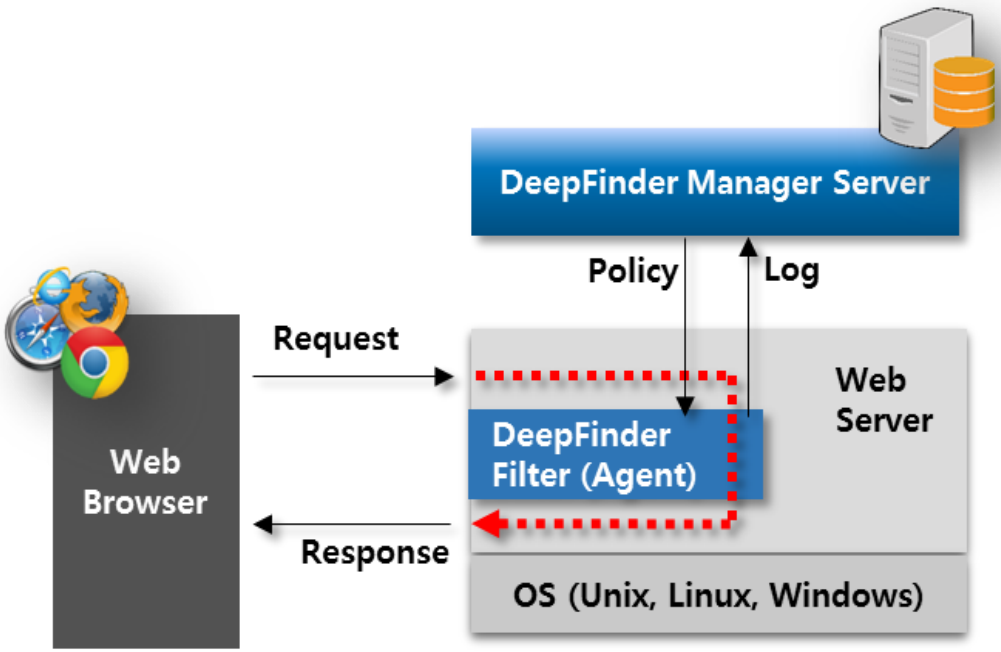
Full SSL Inspection

- 웹 서버가 복호화한 트래픽을 보안 필터링
- 속도 및 성능 저하없이 SSL 암호화 트래픽 분석
- 인증서 갱신 및 관리 필요없음

4. 주요기능

DeepFinder 필터가 웹 서버 내에 설치되어 웹 서버 스스로 보안 동작을 수행합니다.
프록시/네트워크 웹방화벽과 보안성 면에서 차이가 없으며 다양한 보안정책 템플릿을 제공하여 사용자의 필요에 따라 선택 및 수정하여 적용할 수 있습니다.

동작 방식



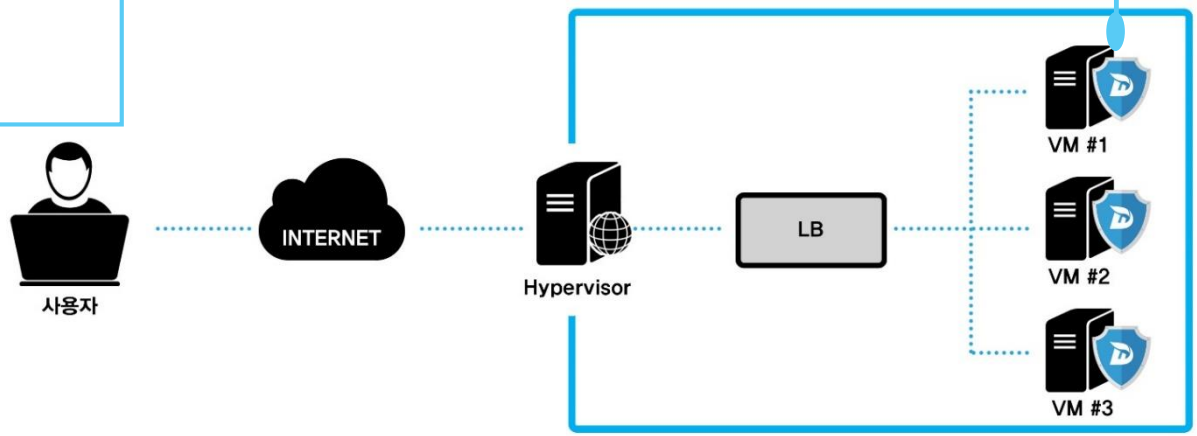
- HTTPS / HTTP/1.0/1.1/2 기반의 웹 공격 대응
- OWASP Top 10, PCI DSS 6.6 요구사항, 국정원 8대 취약점 대응
- Response 데이터 검사 (중요정보 유출 탐지)
- 업로드 파일 검사 : Binary(Rawdata) 시그니처 등록 가능
- 경로별(URI) 파일 위 변조 및 신규 파일 생성 검사 공개 소프트웨어 (제로보드, 테크노트, 그누보드, 공개용 쇼핑몰, 블로그 등)에 대한 보안 정책
- 파일 확장자 우회 업로드 공격 탐지 · 차단
- Layer7 DoS 공격과 무차별 대입 공격 및 사전공격(Dictionary Attack) 탐지 · 차단
- URI 기반 IP 제어 기능 제공 (X-Forwarded-For 식별 가능)
- 웹 기반 매니저 GUI로 누구나 보안 설정 가능
- 리포트 스케줄 제공 (계정별 리포트 자동 생성 및 발송)

Ⅱ. 웹방화벽 특장점

1. 클라우드 환경
2. SSL Inspection
3. Proxy 방식과 비교
4. S/W 웹방화벽과 비교
5. 주요 레퍼런스

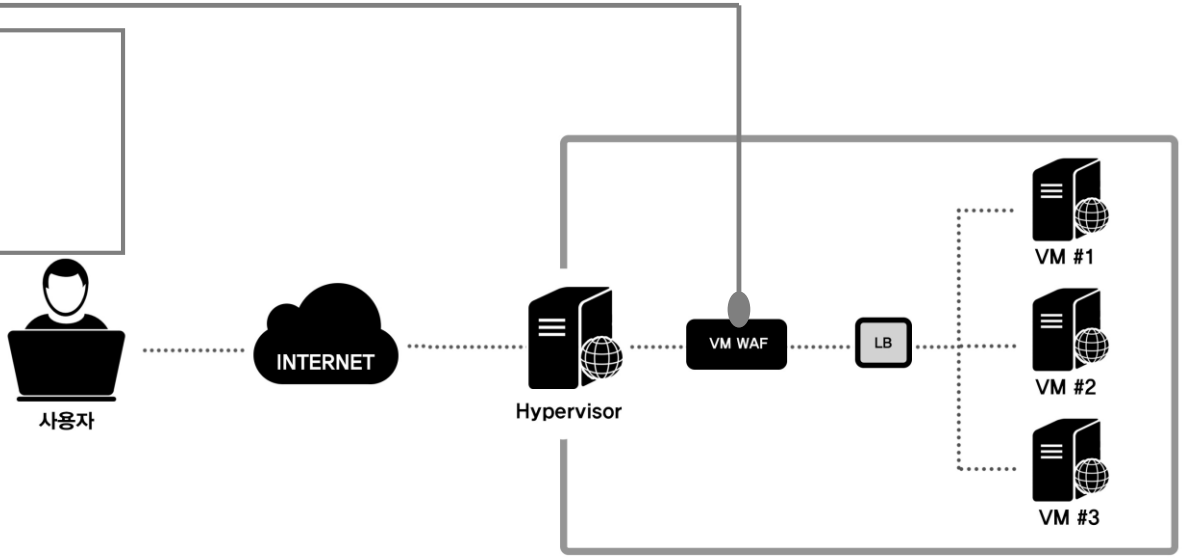
클라우드 웹방화벽(DeepFinder) 사용 시

- 기존 네트워크 변경 없이 그대로 적용(서비스 무중단 Agent 설치)
- 솔루션 자동 확장/삭제 (Auto Scaling)
- 통합 관제 가능 (매니저 Drag&Drop)
- 트래픽량 상관없이 성능 유지 (금액 일정)
- 분산처리로 물리적/논리적 안정성과 고가용성 확보



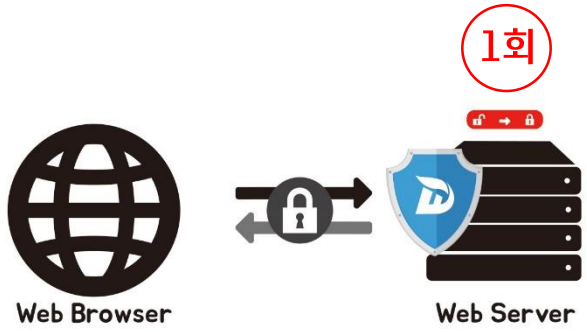
H/W, Proxy 웹방화벽 사용 시

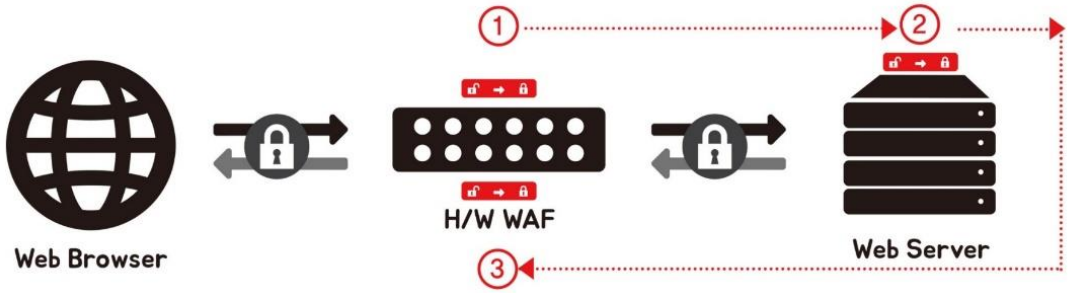
- 웹서버 앞단에 VM 구성
- 환경에 따라 네트워크 변경 필요
- 관제 어려움 (개별 장비이기 때문에 추가 장비 구성 필요)
- 트래픽량에 따라 웹방화벽의 스펙업 필요 (비용 발생)
- 병목현상 (Bottle Neck) 발생



2. SSL Inspection

DeepFinder 는 H/W, Proxy, Reverse Proxy 웹방화벽의 SSL 처리 방식과 달라 가속기 등의 추가 구매 없이, 성능/속도 저하없이 SSL 트래픽을 필터링합니다.





DeepFinder (Filter방식)

웹 서비스 속도 유지하면서 Full SSL Inspection

- DeepFinder는 웹서버 내에서 필터 동작
- 웹 서버가 복호화한 데이터를 검사
- 웹서비스 응답 속도 저하 및 성능 저하 없이 SSL 처리
- 추가 리소스 없이 Full SSL Inspection
- 인증서 관리 불필요

Proxy, Reverse Proxy 방식

속도 저하 및 대용량의 SSL 처리 이슈

- Proxy, Reverse Proxy 방식의 웹방화벽의 경우, 대용량의 SSL 암호화 트래픽이 유입되면 장비 Down 또는 성능 하락 발생 가능
- 이를 방지하기 위한 별도의 SSL가속기 설치 필요 또는 SSL Inspection 기능을 꺼놓기도 함 – 보안 이슈 발생
- 인증서 만료 시점에 맞추어 개별 업데이트 필요

3. Proxy 방식과 비교

H/W / Proxy / Reverse Proxy 웹방화벽과의 차별점

- DeepFinder는 웹 서버 내에 모듈로 설치되기 때문에 웹 서버가 직접 보안 동작을 합니다
- 기존의 네트워크 구성을 바꿀 필요가 없습니다. (Proxy 방식은 네트워크 변경 필요 : 단절 발생)
- 또한 웹 서버가 받은 리퀘스트 중 유효 데이터만 검사하기 때문에 웹 서버의 기존 성능 및 속도에 영향을 주지 않습니다

항목	Filter (DeepFinder)	H/W, Proxy
구성 위치	웹 서버 내 필터(모듈) 동작	웹 서버 앞 단에서 동작
클라우드 환경 구축 시	변경 없이 기존 환경 그대로 적용	클라우드 환경에 따라 커스터마이징 필요
제품 구성	OS, 웹서비스 타입 별 Agent 제공	네트워크, 웹서비스 부하(용량) 별 하드웨어 제공
성능	웹 서버 성능에 따라 다름 시스템 리소스 점유율 (CPU 3% 이내, Memory 약 100M 이하)	제품 라인업별 상이
방어 항목	OWASP Top 10, 국정원 8대 취약점 우회 공격 방어, 내부 공격 방어	OWASP Top 10, 국정원 8대 취약점
웹서비스 속도	유지	병목현상 발생 가능
SSL 처리 방식	웹 서비스가 처리 (Hooking방식) (Filter : 1번 처리)	인증서 복사 필요 (3번 처리)
SSL 처리 속도 (Full Inspection)	속도 저하 없음	감소 (약 5배 느려짐), 가속기 필요
통합 관리	통합 관리 매니저 콘솔 (Drag&Drop) 제공	장비 별 접속
트래픽 처리한계	웹 서버가 다운되지 않는 한 웹방화벽 기능 수행	By-pass (웹방화벽 기능 off)

4. S/W 웹방화벽과 비교

DeepFinder 는 다른 S/W 웹방화벽 대비 다음과 같은 차별성을 제공합니다.

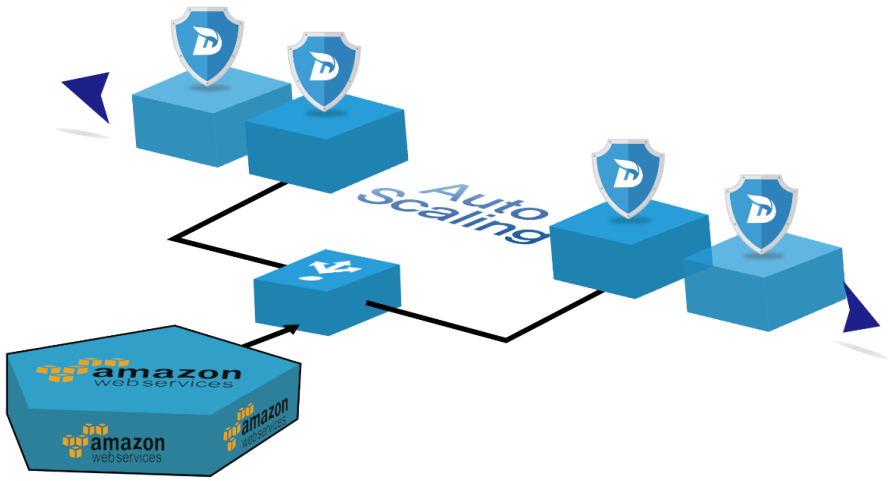
항목	DeepFinder	WebKnight	ModSecurity	DotDefender
지원 웹서버	Apache, IIS, Nginx, WAS	IIS	Apache, IIS, NginX	Apache ,IIS
제공 언어	한글	영문	영문	영문
제공 방식	Manager-Agent	Agent	Agent	Agent
통합 매니저(GUI) 제공	O	X	X	X
자동 보고서	O	X	X	X
보안정책 실시간 관리	O	X	X	X

5. 주요 레퍼런스

LG CNS
AhnLab
SK Infosec
SAMSUNG 에스원
신세계 아이앤씨
NSOK
Cloud Innovator MEGAZONE
gabia.
cafe24
CYBERONE
HOSTWAY GLOBAL WEB SOLUTIONS A 3C COMPANY
WISA.
새정치민주연합
KORAIL 코레일관광개발
한국관광공사 KOREA TOURISM ORGANIZATION
영등포구도시시설관리공단 Yeongdeungpo-Gu Facilities Management Corporate
FKI 전국경제인연합회
군인공제회 MILITARY MUTUAL AID ASSOCIATION
SBS
Cheil
PENGTAI
DAEHONG (주)대홍기획
Ogilvy
SK telecom
LOTTE.com 베트남
ARTBOX
TOSEI
SNUH 분당서울대학교병원
SAMIL 삼일회계법인
netmarble 태국
LG생활건강
THE NORTH FACE
SONO KONG
BBS 불교방송
메가스터디교육그룹 중앙원격평생교육원
참 쉬운 중국어 문정아가 답이다 Since 2003 문정아 중국어
NATURE REPUBLIC
HANBUL Value Creator for Human Beauty
한국화장품
HOLLYS COFFEE
환자가 더욱 행복한 병원 대림성모병원
우아한 형제들
서울우유 서울우유협동조합
한국문학번역원 Literature Translation Institute of Korea
대한예수교침례회총회
대한간호협회 Korean Nurses Association
Kbiz 인천산업유통사업협동조합
성남시청소년재단 SEONGNAM CITY YOUTH FOUNDATION

Ⅲ. 도입사례

1. M IT서비스
2. P 디지털마케팅 에이전시
3. W 대형 e-commerce
4. L SI 회사
5. 중소기업, 소상공인



도입 배경

AWS의 파트너로서 고객사가 필요로 하는 다양한 IT솔루션을 공급하였으나

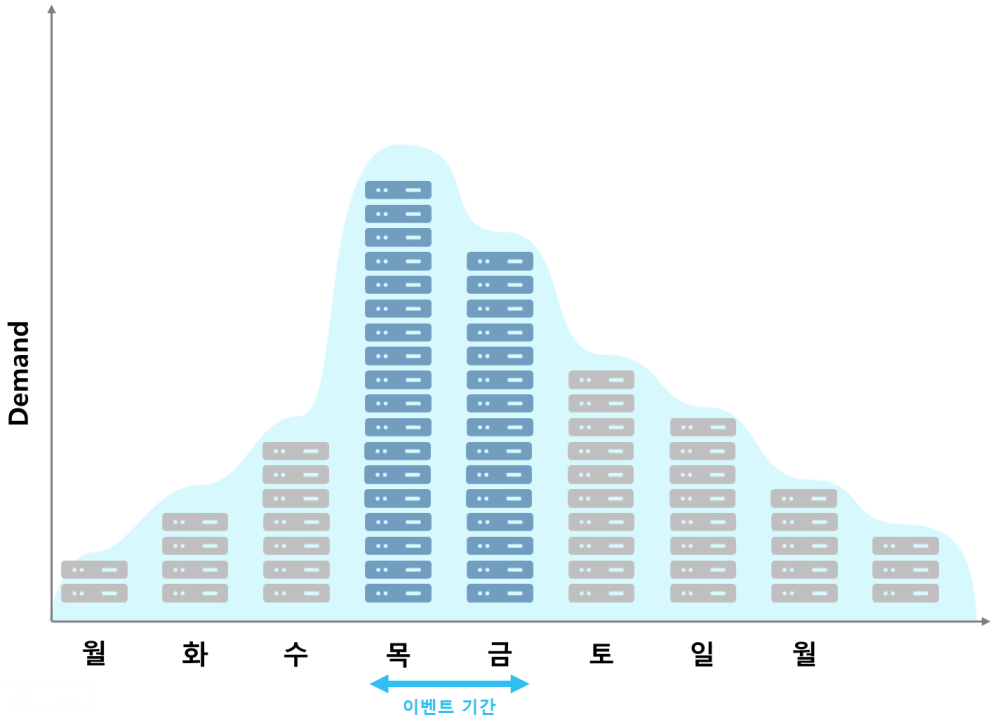
Appliance 타입, Proxy 타입의 웹방화벽으로는 아마존의 AWS환경에 적용하는데

문제점이 많아 클라우드 환경에 최적화된 DeepFinder 를 도입하여

고객사에 24x365 웹 보안 서비스 제공

도입 효과

- Proxy 방식과 달리 별도 인스턴스를 구매할 필요가 없어 비용 절감
- SSL 100% Inspection시 속도 저하 없음
  - 처리 속도, 보안 성능 유지
- AWS의 Auto Scaling 지원하여 보안솔루션도 자동확장, 삭제 / Proxy방식은 Load Balancer의 개수에 따라 운용 서버를 추가 증설하여야 함
- 사용한 만큼만 비용 지불 (시간당 과금 지원)



도입 배경

국내외 디지털 마케팅을 진행하는 회사로 업체 특성상 수시로 이벤트 발생

- 서비스 단절, 서비스 속도에 민감
- 웹 서버 수의 변동폭 큼, 트래픽 변화에 민감

Auto Scaling 을 완벽히 지원하는 웹방화벽 DeepFinder 도입

도입 효과

- 이벤트 기간 동안 이용자 수의 폭발적인 증가에도 단절 없이 서비스
- AWS의 Auto Scaling 완벽 지원
  - 초기 인스턴스 수 (2대) → 이벤트 기간 (120대)
- 사용한 만큼만 사용료 지불 (시간당 과금)
- Proxy 방식과 달리 별도 인스턴스를 구매할 필요가 없어 비용 절감
- 분산처리 및 에이전트 자동화가 가능하여 효율적인 운영

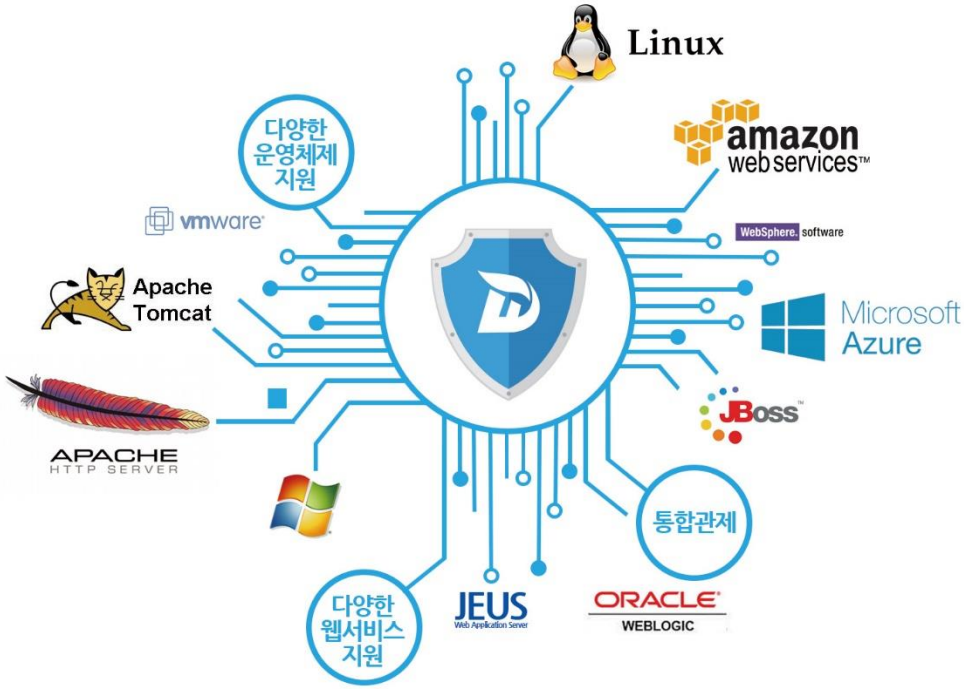
3. W 대형 e-commerce

도입 배경

- AWS로 이전 시 최대 고려사항 : 서비스 무단절, 서비스 속도 유지
- 웹방화벽 BMT 실시 : DeepFinder 필터 타입, 타사 프록시 웹방화벽
- 타사 프록시 대비 평균 3배 이상 빠른 필터타입 DeepFinder 도입
  - test 결과 : (처리속도) 필터 DeepFinder > 타사 프록시)
  - 프록시 웹방화벽 초기 구성 시 서비스 단절 발생
    : 병목현상으로 인해 속도 지연현상 초래 & 서비스 단절타임 발생

도입 효과

- 웹방화벽으로 인한 서비스 단절 및 속도 지연 현상 없이 서비스 중
- 분산된 서비스 환경 및 자동화된 개발 환경을 통합 관리
  (On-premise IDC / Virtual Private Cloud / DevOps)
- AWS의 Auto Scaling, Beanstalk 기능 완벽 지원



도입 배경

해외 지사 등 국내외 다양한 환경의 통합 보안을 위한 솔루션이 필요하여

Appliance 웹방화벽과 DeepFinder 에 대한 BMT 를 실시.

클라우드 환경에 최적화된 DeepFinder 를 최종 선정하여 신속한 장애 대응 체계 구축

도입 효과

- 위치, OS의 종류, 웹서버의 종류에 관계없이 통합 보안 구현
- AWS, 자사 Cloud 등 Pivate/Public Cloud 모두 대응
- H/W 웹방화벽 대비 투입 인원, 비용 절감

5. 중소기업, 소상공인

F 온라인 쇼핑몰

J 성형외과

P 여행사

도입 배경

웹 서비스를 하면서 회원정보 및 주민등록번호, 신용카드, 의료기록 등의 중요 정보를 취급함
웹 보안의 중요성을 알지만 사내 보안 전문가 없음. 비용 및 유지 관리에 대한 부담이 있었음
경제적이고 보안 성능도 탁월한 DeepFinder 도입

도입 효과

- 중소기업에도 부담 없는 서비스 이용료
- 노후화 및 업그레이드 비용 부담 감소 (H/W 대비)
- 보안관제 전문팀이 24시간 관제서비스 무상지원

Ⅳ. 지원범위

1. 지원범위
2. 시스템 최소 요구사항

1. 지원범위

※ DeepFinder 가 지원하는 웹 서버 버전, bit, Kernel 버전, Java 버전, WAS 버전 등 지원 가능한지 확인하십시오.

※ 커스터마이징된 환경의 경우, 설치 전 시스템 확인 작업이 필요합니다.

※ 서비스 재시작이 필요한 웹서버 - WAS (JEUS, Tomcat 등) | IIS 6.0 이하 버전 (6.0에 재생 기능이 있으나 간혹 Agent 연결이 불가한 경우)

Operating System	Web Servers / WAS (Web Application Servers)
Microsoft Windows 2003, 2008, 2012, 2016	• IIS 6.0, IIS 7.0, IIS 8.0, IIS 10 • Apache 2.0, 2.2, 2.4 • Java EE6 이상 인증서버 – Tomcat, Jeus, WebLogic, WebSphere ※ WAS Agent의 경우 Server 2008 이상만 지원
Intel Linux Kernel 2.6.x 이상 32bit, 64bit	• Apache 2.0, 2.2, 2.4 • NGINX 1.8.1, 1.10.X 이상 • Java EE6 이상 인증서버 – Tomcat, Jeus, WebLogic, WebSphere

2. 시스템 최소 요구사양

※ DeepFinder는 웹 서버 내부에서 Filter(모듈)이 동작하는 방식이기 때문에 DeepFinder의 성능은 설치된 웹 서버의 성능을 따라갑니다.

Module	System Requirements	
DeepFinder Manager	CPU	2GHz (2Core 이상)
	Main Memory	8GB
	HDD	500G
	OS	Linux 계열 O/S 플랫폼 (CentOS 6 선호)
DeepFinder Agent	Main Memory	4GB
	HDD	100 MB
	OS	WAS, APACHE, IIS 가 구동되는 모든 OS
	Web Server	IIS 6.0, 7.0, 8.0, 10.0 Apache 2.0~ 2.4 NginX 1.8.10~ 1.10.2
	Web Application Server (WAS)	Servlet 3.0 JavaEE 6 Java EE6 이상 인증을 획득한 WAS Server

감사합니다.

DOUZONE
www.douzoneon.com

Maximizing
Potential