SonicWALL Capture ATP

SMB 전용 APT 솔루션

SonicWALL Korea

SONICWALL™

1. 진화하는 보안 위협 APT

1. 국내 주요 해킹피해 사례

SONICWALL

APT 보안 위협은 예전에도 있었고,
지금도 있으며, 앞으로도 있을 것입니다.

2008년
GS 칼텍스 1125만 회원정보유출
하나로텔레콤 600만 고객정보유출
옥션 1863만 개인정보유출
2009년
7.7 DDoS 대란
정부기관, 포털 마비
2010년
신세계몰 820만 개인정보유출

3월, SKT/KT
20만 개인정보유출
5월, EBS
400만 개인정보유출
7월, KT
870만 개인정보유출

1월, KB국민은행/롯데카드/NH농협
2000만 개인정보유출
3월, 국토교통부
2000만 개인정보유출
12월, 한국수력원자력
내부문서유출

7월, 인터파크
1030만 개인정보유출

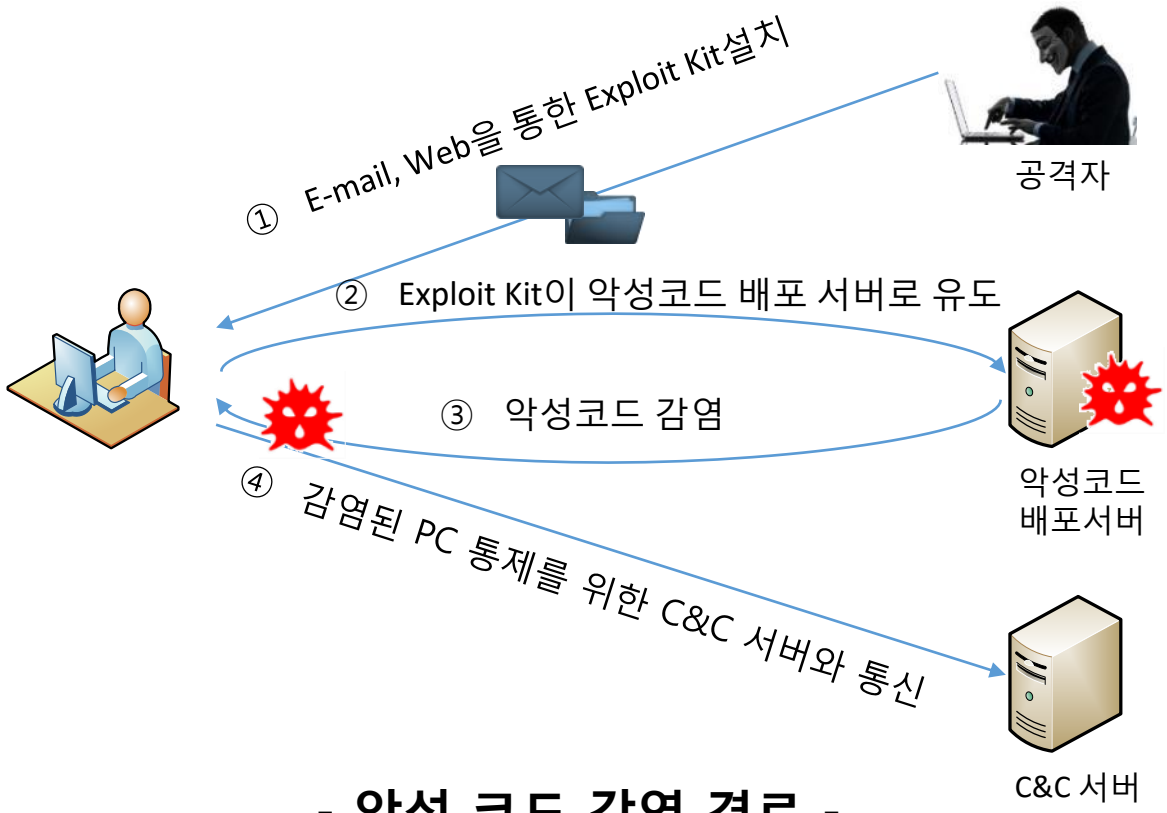
~2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016

3월, 3.3 DDoS
정부기관, 은행 마비
4월, 현대캐피탈
175만 개인정보유출
4월, 농협
전산망 마비
7월, SK 컴즈
3500만 개인정보유출
11월, 넥슨
1320만 개인정보유출

3월, 3.20 전산대란
MBC/KBS/신한은행/농협
전산망 마비
5월, 민족문제연구소
912만 개인정보유출
6월, 6.25 사이버테러
새누리당/군장병/청와대/
주한미군 294만 개인정보유출

3월, 아이핀
75만건의 아이핀 부정 발급

2. 진화하는 APT



- 악성 코드 감염 경로 -

```
function gs7sfd(txt) {
    var v1 = 'XM' + 'LD' + 'OM',
    v2 = 'pa' + 'rseE' + 'rr' + 'or',
    v3 = 'loa' + 'dX' + 'ML',
    v4 = 'DT' + 'D X' + 'HTML 1.0 Transitional',
    v5 = 'err' + 'orC' + 'ode';
    var resInf = new ActiveXObject("Microsoft." + v1),
    subpath = "c:\\Windows\\System32\\drivers\\" + txt + ".sys";
    resInf.async = true;
    resInf[v3]('&lt;!DOCTYPE html PUBLIC "-//W3C//' + v4 + '//EN" "res://' + subpath + '"&gt;');
    if (resInf[v2][v5] != 0) {
    return 0;
}
var tmp;
try {
    tmp = new ActiveXObject('Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi.1');
} catch (e) {
    tmp = false;
}
if (tmp || gs7sfd("kl1") || gs7sfd("tmactmon") || gs7sfd("tmcomm") || gs7sfd("tmevtmgr") || gs7sfd("TMEBC32") || gs7sfd("tmeext") || gs7sfd("tmnciesc") || gs7sfd(
"tmtdi") || gs7sfd("vm3dmp") || gs7sfd("vmusbmouse") || gs7sfd("vmmouse") || gs7sfd("vmhgfs") || gs7sfd("VBoxGuest") || gs7sfd("VBoxMouse") || gs7sfd("VBoxSF") ||
gs7sfd("VBoxVideo") || gs7sfd("prl_boot") || gs7sfd("prl_fs") || gs7sfd("prl_kmdd") || gs7sfd("prl_memdev") || gs7sfd("prl_mouf") || gs7sfd("prl_pv32") || gs7sfd(
"prl_sound") || gs7sfd("prl_strg") || gs7sfd("prl_tg") || gs7sfd("prl_time")) {
    Target();
} else {
    function Check(s) {
```

txt is the argument passed to this function

Checking for files related to VMware, virtual box

Checking for files related to Kaspersky, TrendMicro Anti-virus

Checking for files related to Parallels software

- Exploit KIT code 탐지 회피 방법 -

- 실제 공격 PC의 공격가능한 취약점 분석(OS, 브라우저, Flash 버전 등)
- 공격 PC에 백신의 설치, 가상 환경 여부 확인

✓ **가장 적절한 공격 방법을 결정**하고 악성코드를 설치하기 위해 공격 대상의 환경에 따라 다른 공격을 실행

3. 보안 위협의 다양화 및 증가

- 다양한 Malware의 출현과 폭발적인 증가 -

- 공격 대상의 증가-

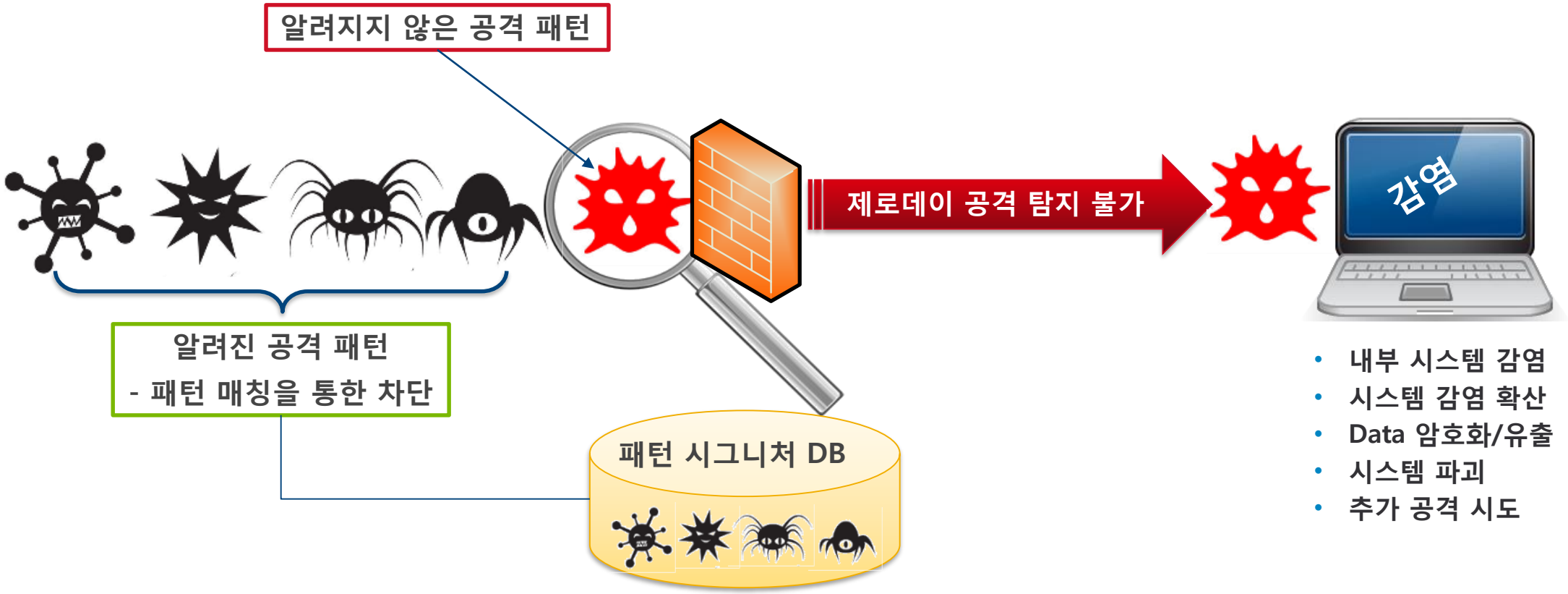
- 다양한 단말과 OS를 대상으로 공격 범위가 확대
- 해커들의 조직화로 많은 Malware 출현
- 2014년 대비 2015년 Malware의 수가 약 70% 증가
- 기존 Malware의 간단한 Code 수정을 통한 수 많은 변종 생성

✓ **APT공격의 핵심은 Zero-day 공격**으로 알려지지 않은 패턴을 의미
매일 새로운 보안 위협으로부터 기업 자산을 보호해야 함

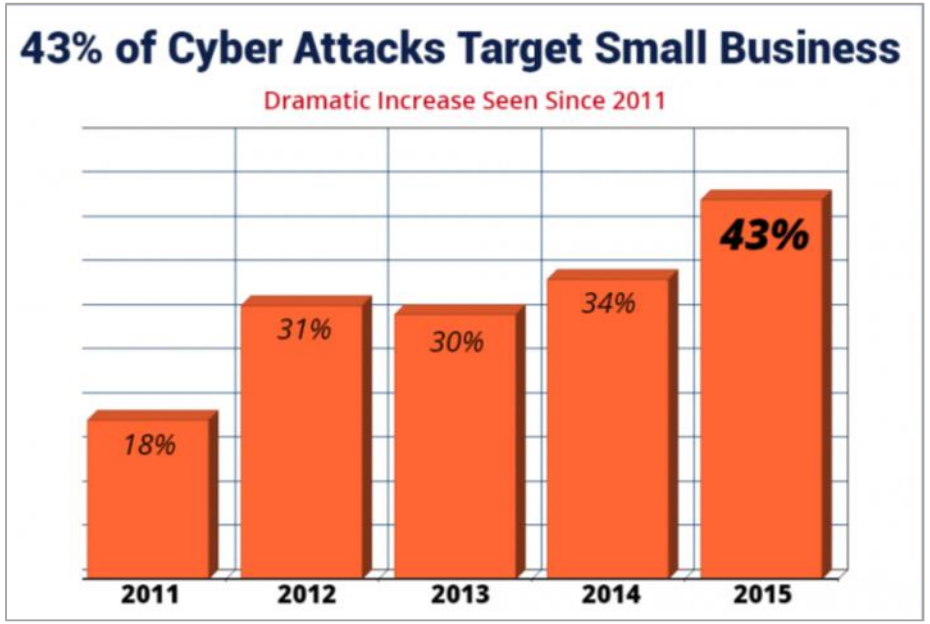
4. Zero-day 공격의 위험성

SONICWALL™

✓ **Zero-day 공격은 알려지지않은 새로운 보안 위협으로** 기존의 패턴 시그니처 매칭 방식의 보안 솔루션는 대응이 불가능하며, APT공격의 중요한 수단으로 사용이 되고 있다. 때문에 **새로운 악성코드의 행위를 분석하고 판단 할 수 있는 솔루션이 필요**하다.



5. 국가기관, 대기업만 노린다?



- 중,소규모 기업을 대상으로 하는 공격은 매년 증가하고 있다. (2015년 해킹의 43%가 SMB를 목표로 함)
- 근래 Ransomware와 같이 불특정 다수를 노리는 Malware가 많이 등장
- Zero-day 공격으로 언제 어디서라도 보안 사고는 일어날 수 있음

✓ 기업의 규모가 작아도 지켜야 할 기업 자산이 있다면 Zero-day 공격에 대한 방안이 있어야 합니다 .
이제는 **중소기업도 APT에 대한 솔루션을 고려해야 할 시기입니다**.

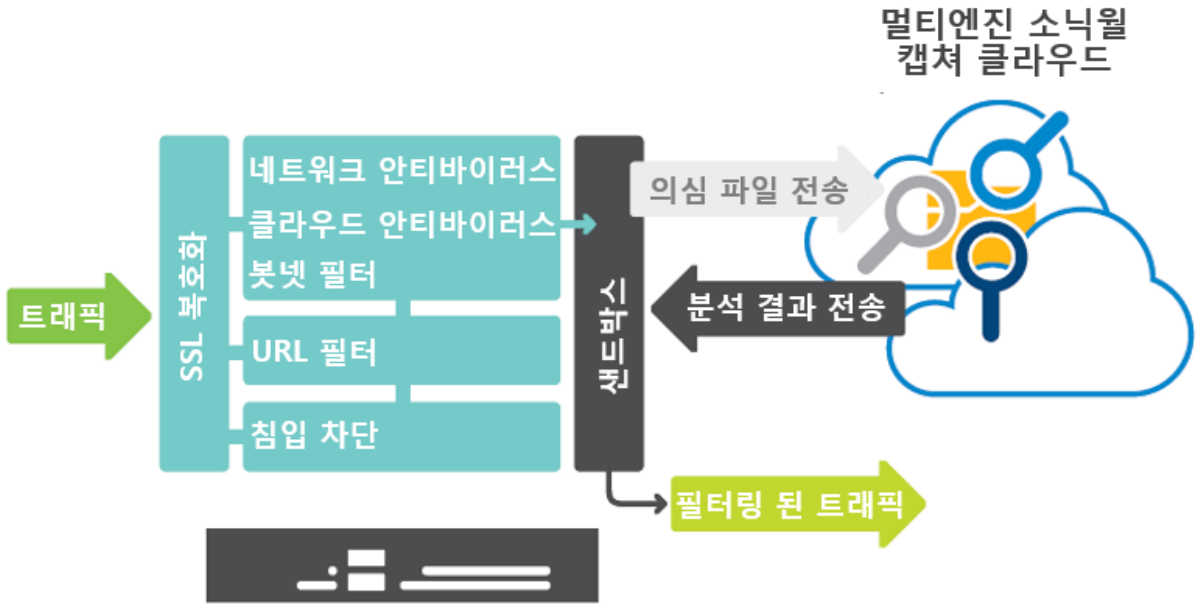
SONICWALL™

2. SonicWALL Capture ATP 소개

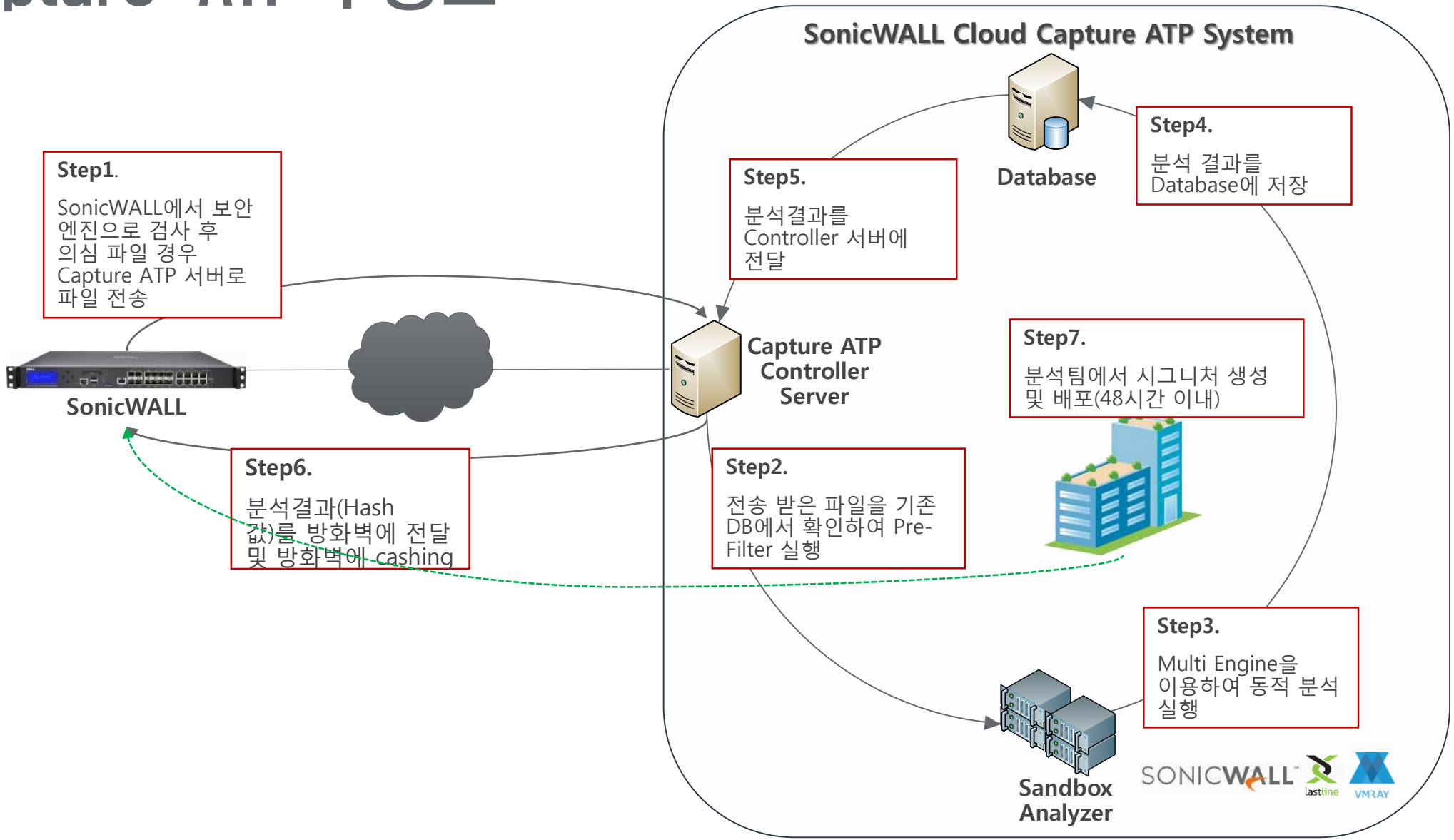
1. Capture ATP 개요

「**SonicWALL의 Capture 서비스는 Zero-day 공격에 가장 효과적인** sandboxing 기법을 Cloud 형태로 제공을 하며, 방화벽과의 연동을 통해 간단하게 APT에 대한 위협을 제거합니다」

- **멀티엔진 기반의 지능화 된 위협 분석은 위협 탐지가 뛰어나고, 악성코드의 회피를 어렵게 한다.**
  - Virtualized sandbox
  - Full system emulation
  - Hypervisor level analysis
- **다양한 파일 유형과 OS 환경 분석 지원**
  - PE, MS Office, PDF, archives, JAR, APK
  - Windows, Android and Mac OS (H216)
- **Block until verdict(평가 대기) 기능**
- **개선된 Signature의 신속한 배포**
- **자동 및 수동 파일 제출 및 분석**



2. Capture ATP 구성도



3. Multi Engine

SONICWALL™

Sonic Sandbox

SONICWALL™

Hypervisor 레벨 분석

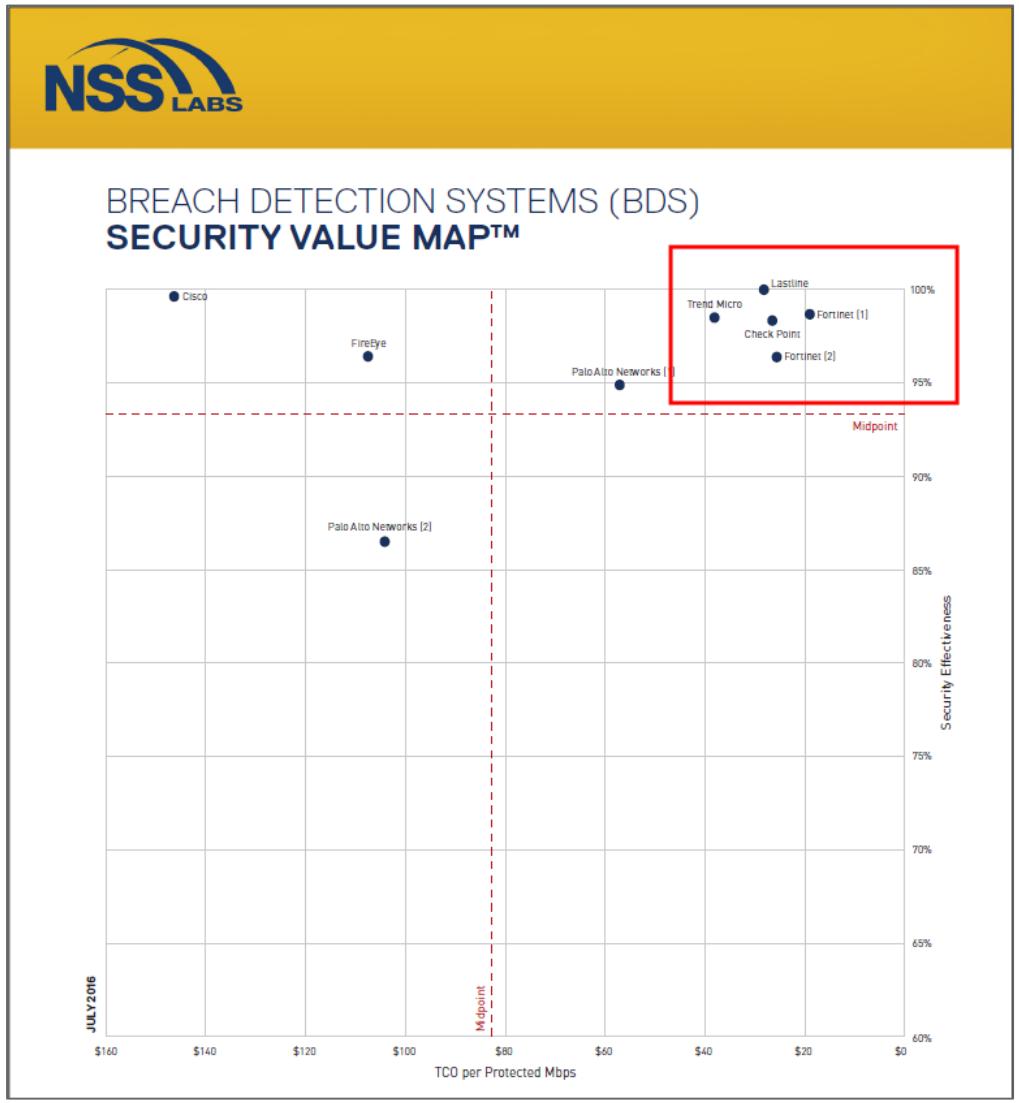
VMRAY

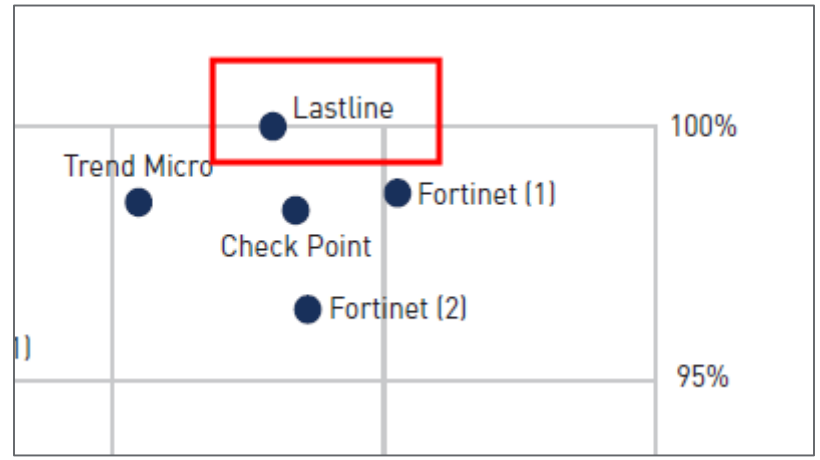
Full System Emulation

lastline

Capture ATP는 멀티엔진 기반의 Sandbox 분석을 지원하여 **탐지율이 뛰어나고 악성코드의 탐지 회피를 어렵게** 합니다.

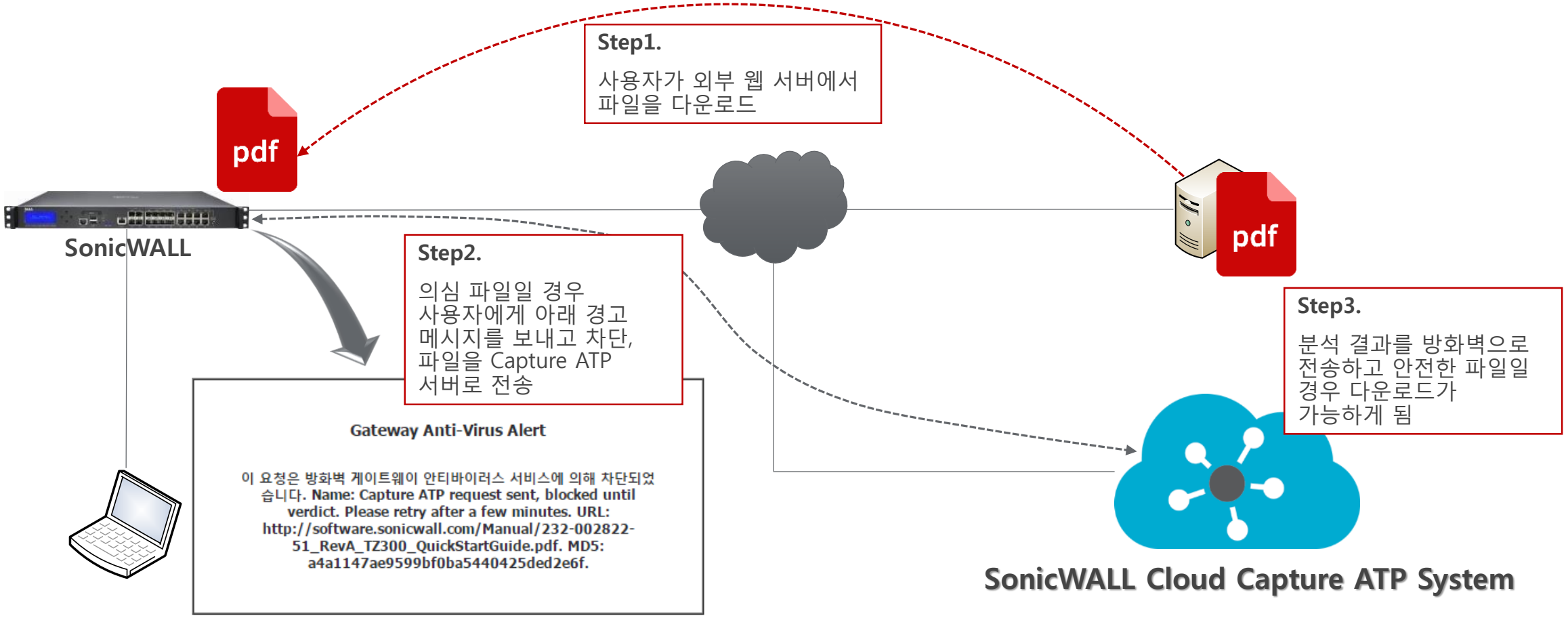
3. Multi Engine





소닉월의 멀티 엔진 중 하나인 Lastline은 **2016년 NSS LABS Breach Detection Systems (BDS) 부분에서 최고의 탐지율**을 보여 우수한 APT 탐지 성능을 확인

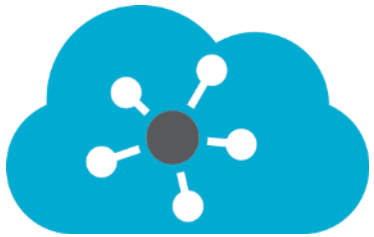
4. 평가 대기 기능



Capture ATP의 평가 대기 기능은 **의심파일을 분석하는 동안 해당 파일의 내부 유입을 막는 기능**으로,
보다 강력한 보안 정책을 수립 할 수 있다.

5. 간단한 구성 및 운영

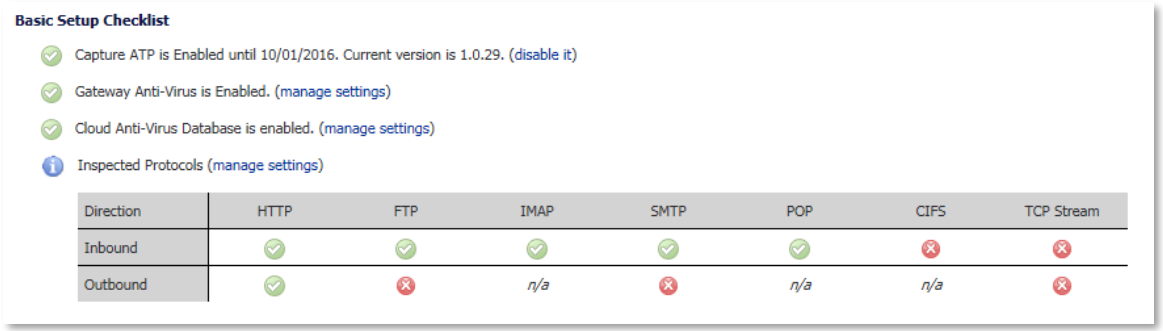
SONICWALL™



SonicWALL Capture ATP System

SonicWALL Device

- SonicWALL 장비와 Cloud 연동의 **심플한 구성**
- 간단한 설정을 통한 **쉬운 운영**



Basic Setup Checklist

Capture ATP is Enabled until 10/01/2016. Current version is 1.0.29. (disable it)

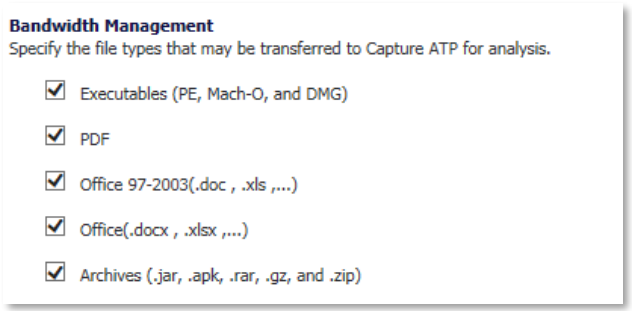
Gateway Anti-Virus is Enabled. (manage settings)

Cloud Anti-Virus Database is enabled. (manage settings)

Inspected Protocols (manage settings)

Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✓	✓	✓	✓	✓	✗	✗
Outbound	✓	✗	n/a	✗	n/a	n/a	✗

- 탐지 프로토콜 설정-

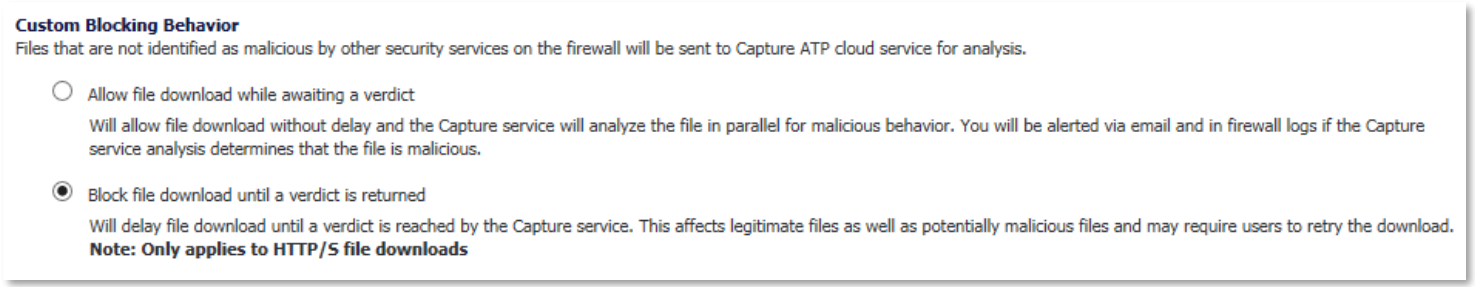


Bandwidth Management

Specify the file types that may be transferred to Capture ATP for analysis.

- [x] Executables (PE, Mach-O, and DMG)
- [x] PDF
- [x] Office 97-2003(.doc , .xls ,...)
- [x] Office(.docx , .xlsx ,...)
- [x] Archives (.jar, .apk, .rar, .gz, and .zip)

- 탐지 파일 유형 설정-



Custom Blocking Behavior

Files that are not identified as malicious by other security services on the firewall will be sent to Capture ATP cloud service for analysis.

- ○ Allow file download while awaiting a verdict

  Will allow file download without delay and the Capture service will analyze the file in parallel for malicious behavior. You will be alerted via email and in firewall logs if the Capture service analysis determines that the file is malicious.

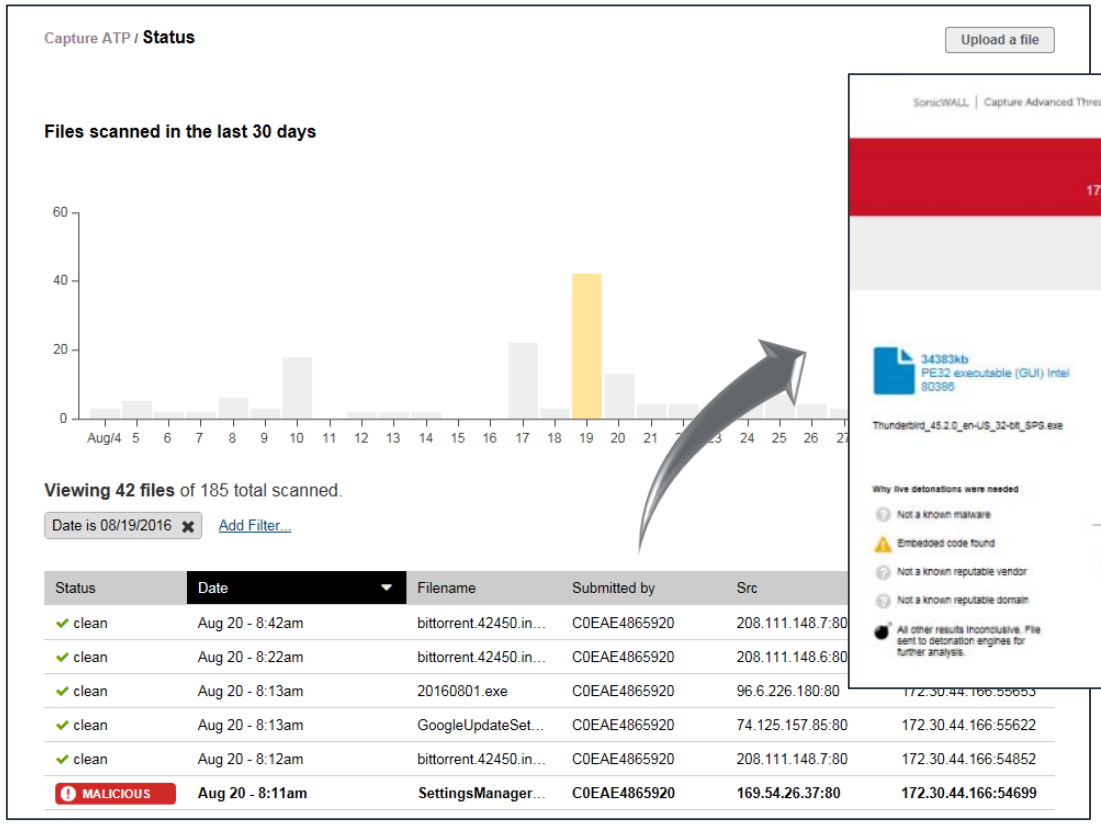
- ◉ Block file download until a verdict is returned

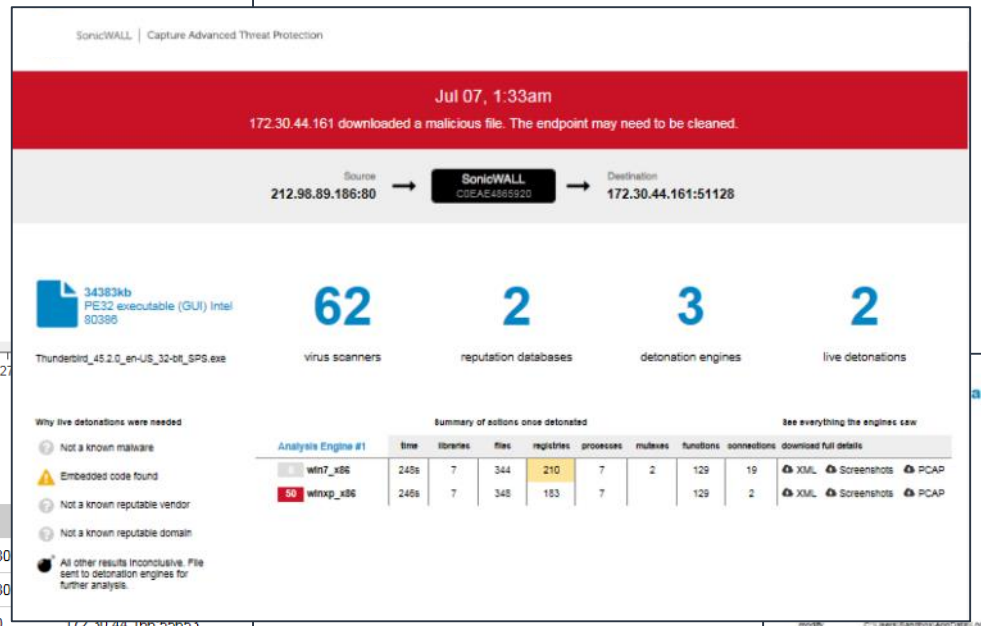
  Will delay file download until a verdict is reached by the Capture service. This affects legitimate files as well as potentially malicious files and may require users to retry the download.
  Note: Only applies to HTTP/S file downloads

- 차단 방식 설정-

6. 분석 보고서

- 각 파일의 분석 보고서를 통한 위협 확인





- 한 달간의 File 분석 현황 보고서 지원
- 일별 탐지 파일 통계 및 기간 Filter 제공
- 사용자 Upload 기능으로 Local 파일 위협 분석

- 악성코드의 상세 행위 분석 보고서 및 Screenshot 제공

7. Capture 적용 모델

SonicWALL Line up							
Model	**SOHO**	**TZ300**	**TZ400**	**TZ500**	**TZ600**	**NSA2600**	**NSA3600**
CPU	2x 400MHz	2x 800MHz	4x 800MHz	4x 1 GHz	4x 1.4 GHz	4x 800MHz	6x 800MHz
Memory	512 MB	1GB	1GB	1GB	1GB	2GB	2GB
Interfaces	1Gbe Copper *5	1Gbe Copper *5	1Gbe Copper *7	1Gbe Copper *8	1Gbe Copper *10	8x1GbE, 1GbE Management, 1 Console	2x10GbE SFP+, 4x1GbE SFP, 12x1GbE,1GbE Management, 1 Console
Firewall Throughput	300M	750M	1.3G	1.4G	1.5G	1.9G	3.4G
IPS Throughput	100M	300M	900M	1.0G	1.1G	700M	1.1G
Anti-Malware inspection Throughput	50M	100M	300M	400M	500M	300M	500M
VPN Throughput	100M	300M	900M	1.0G	1.1G	1.1G	1.5G
Maximum Connections	10K	50K	100K	125K	150K	225K	325K
New Sessions/Sec	1,800	5,000	6,000	8,000	12K	15K	20K
Capture ATP	**N/A**	✓	✓	✓	✓	✓	✓
Model	**NSA4600**	**NSA5600**	**NSA6600**	**SM9200**	**SM9400**	**SM9600**	**SM9800**
CPU	8x 1.1GHz	10x 1.3GHz	24x 1.0GHz	24x 1.0GHz	32x 1.2GHz	32x 1.2GHz	64x 1.2GHz
Memory	2GB	4GB	4GB	8GB	16GB	32GB	64GB
Interfaces	2x10GbE SFP+, 4x1GbE SFP, 12x1GbE,1GbE Management, 1 Console	2x10GbE SFP+, 4x1GbE SFP, 12x1GbE,1GbE Management, 1 Console	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE,1GbE Management, 1 Console	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE,1GbE Management, 1 Console	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE,1GbE Management, 1 Console	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE,1GbE Management, 1 Console	4x10GbE SFP+, 12x1GbE SFP, 8x1GbE,1GbE Management, 1 Console
Firewall Throughput	6.0G	9.0G	12G	10G	20G	20G	40G
IPS Throughput	2.0G	3.0G	4.5G	5.0G	10G	11.5G	24G
Anti-Malware inspection Throughput	800M	1.6G	3.0G	3.5G	4.5G	5.0G	10G
VPN Throughput	3.0G	4.5G	5.0G	5.0G	10G	11.5G	18G
Maximum Connections	400K	562.5K	750K	1.25M	1.25M	1.5M	3.0M
New Sessions/Sec	40K	60K	90K	100K	130K	130K	280K
Capture ATP	✓	✓	✓	✓	✓	✓	**TBD**

SONICWALL™

3. 기능 비교 및 효과

1. APT 솔루션 비교

ATP 솔루션 비교						
Vendor	**구성 플랫폼**	**Sandbox 형태**	**OS 환경**	**지원 프로토콜**	**지원 파일 유형**	**평가 대기**
FireEye	Standalone (Inline or out of band)	Virtual	Windows, Mac	HTTP/S, FTP, SMTP	PE, MS office, PDF, Arch, JavaScript, Flash, JAR, RAR media, URLs	
paloalto NETWORKS	Standalone / Integrated cloud service	Virtual, network and endpoint	Windows, Android, Mac	HTTP/S, FTP, SMTP, IMAP, POP3	PE, MS office, PDF, Arch, JavaScript, Flash, JAR, APK, URL image, SMB	
Check Point SOFTWARE TECHNOLOGIES LTD.	Standalone / Integrated cloud service	Virtual, CPU emulation	Windows	HTTP/S, SMTP	PE, MS Office, PDF, Arch, Flash, Java, PIF	
SONICWALL	Integrated cloud service	**Virtual, Full system emulation, Hypervisor layer analysis**	**Windows, Android**	**HTTP/S, FTP, SMTP, IMAP, POP3, CIFS**	PE, MS office, PDF, JAR, APK, RAR, gz, zip	**HTTP/S**

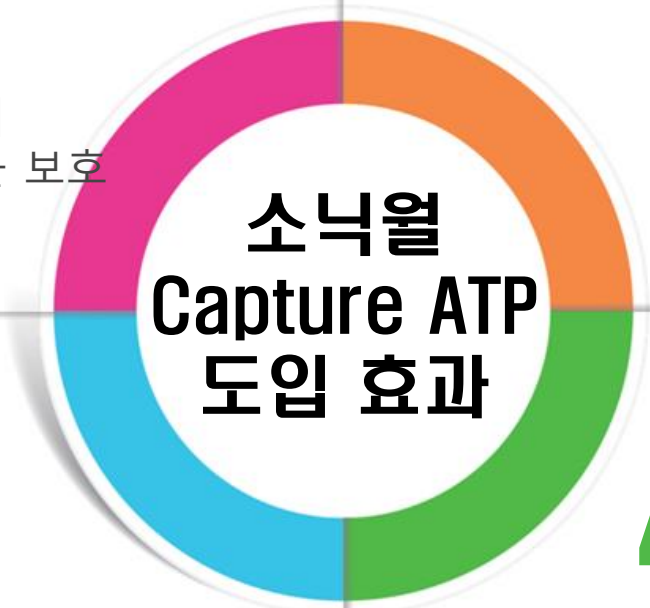
2. Capture 도입 효과

1. 높은 보안 효과

멀티엔진의 Sandbox는 탐지율이 뛰어나고, 점점 지능화되고 있는 악성코드의 탐지 회피를 어렵게 하여 Zero day 공격으로 부터 기업 자산을 보호

2. 낮은 TCO

국가기관, 대기업에서 도입하는 고가의 Appliance가 아닌 Cloud형태의 서비스를 통한 APT 차단 솔루션으로 도입 비용이 낮음



3. 간단한 구성

SonicWALL 보안 장비와 Cloud Capture시스템의 연동만으로 구성 하기 때문에 기업 네트워크에 복잡도가 적음

4. 쉬운 운영, 분석 보고서

간단한 설정만으로 APT기능 사용이 가능하고, 파일의 행위분석 보고서를 제공하여 보안 위협에 대한 가시성 제공

Thank you!