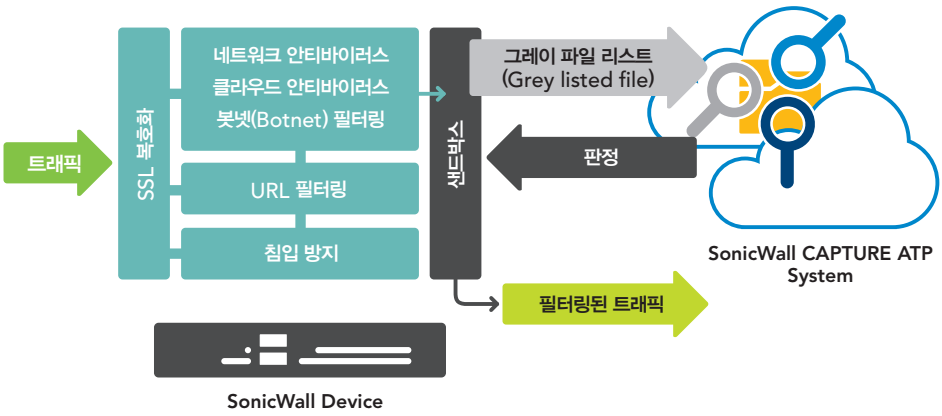
소닉월 CAPTURE
- APT 방어 전용 솔루션

지능형 위협 차단 샌드박스의 효과 대폭 향상

멀티엔진 SonicWall Capture 클라우드



게이트웨이에서 알려지지 위협과 제로데이 공격을 차단하는 클라우드 기반의 다중 엔진 솔루션

- 우수한 보안 효과
- 빠른 응답 시간
- TCO 감소
- 멀티 엔진 샌드박싱 기술
- 다양한 형식의 파일 분석
- 파일 크기 제한 없음

기업들은 효과적으로 제로데이 공격을 차단하기 위하여 악성 코드 분석 기술이 탑재된 솔루션을 도입해야 하며, 이를 통해 파악하기 어려운 위협과 악성코드를 차단할 수 있습니다.

증가하는 제로데이 공격으로부터 고객을 보호하기 위해 SonicWall 방화벽과 연동되는 클라우드 기반의 SonicWall Capture ATP(Advanced Threat Protection) Service는 게이트웨이에서 지능형 위협을 감지하고, 유해성 여부를 판단할 때까지 차단할 수 있습니다. 이 서비스는 풀 시스템 에뮬레이션 (full system emulation)과 가상화 기술을 탑재한 멀티 레이어 샌드박싱(Multi-layer candboxing)으로 의심스러운 코드 행위를 분석할 수 있는 업계 유일의 지능형 위협 차단 솔루션입니다.

이러한 강력한 조합은 단일 엔진 샌드박스 솔루션보다 다양한 위협을 감지할 수 있으므로, 우회 공격에 취약한 컴퓨팅 환경에서 사용하기 적합합니다.

SonicWall Capture ATP Service는 트래픽을 스캔하여 분석할 필요가 있는 의심스러운 코드를 가려내며, 다른 게이트웨이 솔루션들과 달리 분석이 필요한 파일 사이즈의 제한이 없습니다. Global threat intelligence infrastructure는 추가적인 침투를 방지할 수 있도록 새롭게 확인된 시그니처를 모든 SonicWall 네트워크 보안 장비에 신속하게 배포하며, 고객은 높은 수준의 보안, 빠른 응답시간, TCO 감소 효과를 누리실 수 있습니다.

특징

다중 엔진 지능형 위협 분석

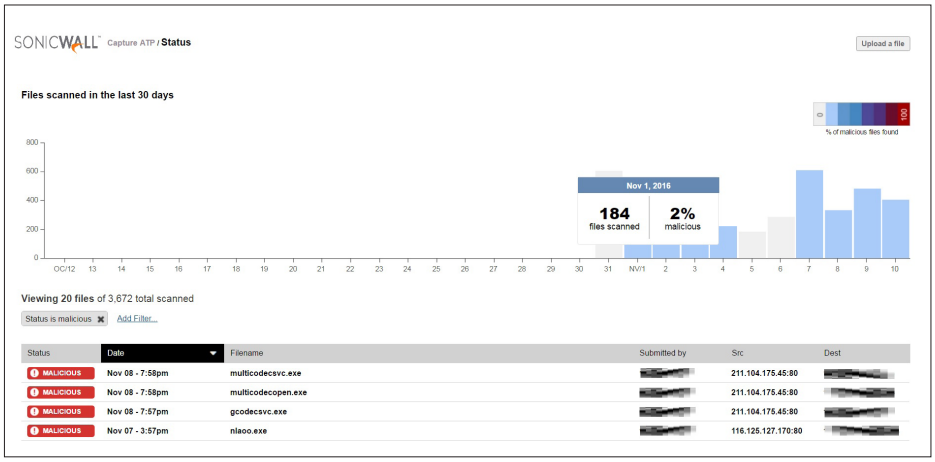
SonicWall Capture ATP Service는 방화벽의 위협 차단 범위를 확대하여 제로데이 공격 및 악성 코드를 감지하고 차단합니다. SonicWall 방화벽은 트래픽을 검사하여 기존 멀웨어를 포함한 각종 침입을 감지하여 차단하며, 의심스러운 파일은 분석을 위해 SonicWall Capture clould service로 전송됩니다. 가상 샌드박싱, 풀 시스템 에뮬레이션과 하이퍼바이저 계층의 분석 기술이 탑재된 멀티 엔진 샌드박스 플랫폼은 미심쩍은 코드를 실행하려 행위를 분석하고 악의적 활동에 대한 포괄적인 가시성을 제공하는 한편, 우회 전략을 무력화하고 제로데이 위협 감지를 극대화합니다.

다양한 형식의 파일 분석 및 파일 크기 제한 없음

SonicWall Capture ATP Service는 Windows, Android, Mac OSX를 비롯한 여러 운영체제 외에도 실행 프로그램(PE), DLL, PDF, MS Office 문서, Archives, JAR, APK 등 다양한 유형의 파일을 크기 제한 없이 분석할 수 있습니다. 관리자는 파일의 유형, 크기, 발신자, 수신자 또는 프로토콜 등 클라우드에 전송해서 분석할 파일을 선택 또는 제외함으로써 분석 대상을 맞춤 설정할 수 있으며, 관리자가 분석할 파일을 클라우드 서비스에 수동으로 전송할 수도 있습니다.

멀티 엔진기반의 지능형 위협 분석 기능

✓ Virtual Sandboxing (SonicWall)
✓ Hypervisor 레벨 분석 (VMRAY)
✓ Full System Emulation (Lastline)



SonicWall Capture ATP Service 상태 페이지에는 최근 30일간 분석을 위해 전송한 파일 개수와 악성으로 판정된 파일의 비율을 한눈에 알 수 있는 막대그래프가 표시됩니다. File history table에는 검사한 파일, 분석 판정 결과, 전송지 및 목적지가 열거됩니다. 구체적인 날짜, 파일 상태, 파일명, 출발지 또는 목적지를 기준으로 빠르게 검색할 수 있는 상세 검색 기능도 지원됩니다. 파일을 선택하면 세부적인 파일 분석 보고서가 표시됩니다.

유해성 판정이 내려질 때까지 차단

잠재적 악성 파일이 네트워크에 유입되는 것을 방지할 수 있도록 클라우드 서비스에 전송한 파일의 유해성 판정이 내려질 때까지 파일의 유입을 게이트웨이에서 보류할 수 있습니다.

신속한 시그니처 배포

파일이 악성으로 판정된 경우 후속 공격을 차단할 수 있도록 시그니처를 즉시 방화벽에 적용할 수 있습니다. 또한 악성 코드는 SonicWall 위협 인텔리전스 팀에게 전달되어 추가 분석을 실시하고 위협 정보를 게이트웨이 안티바이러스 및 IPS 시그니처 데이터베이스에 추가됩니다. 뿐만 아니라 48시간 내에 URL, IP 및 도메인 데이터베이스에도 위협 정보가 전송됩니다.

보고서 및 알림

SonicWall Capture ATP Service는 악성 코드가 활성화된 이후의 활동 내역 외에도, 전송지, 목적지, 요약 정보와 더불어 클라우드 서비스에 전송된 파일의 세부적인 분석 결과를 한눈에 알 수 있는 위협 분석 대시보드와 보고서를 제공합니다. 또한 방화벽 로그 알림 기능은 SonicWall Capture ATP Service는 전송된 미심쩍은 파일과 파일 분석 결과가 포함된 메시지를 전송합니다.

제품 세부 사양

Model	TZ300	TZ400	TZ500	TZ600	NSA2600	NSA3600	NSA4600	NSA5600	NSA6600	SM9200	SM9400	SM9600
PERFORMANCE												
Firewall Throughput	750M	1.3G	1.4G	1.5G	1.9G	3.4G	6.0G	9.0G	12G	15G	20G	20G
Threat Prevention Throughput	300M	900M	1.0G	1.1G	700M	1.1G	2.0G	3.0G	4.5G	5.0G	10G	11.5G
Full DPI(Anti Virus) Throughput	100M	300M	400M	500M	300M	500M	800M	1.6G	3.0G	3.5G	4.5G	5.0G
IPSecVPN Throughput	300M	900M	1.0G	1.1G	1.1G	1.5G	3.0G	4.5G	5.0G	5.0G	10G	11.5G
Maximum Sessions	50K	100K	125K	150K	225K	325K	400K	562.5K	750K	1.25M	1.25M	1.5M
New Connections/Sec	5,000	6,000	8,000	12K	15K	20K	40K	60K	90K	100K	130K	130K
IPSecVPN Tunnel	10	20	25	50	75	800	1500	4000	6000	10,000	10,000	10,000
IPSecVPN Client(Max)	10	25	25	25	250	1,000	3,000	4,000	6,000	4,000	6,000	10,000
SSL VPN Client(Max)	50	100	150	200	250	350	500	1,000	1,500	3000	3000	3000
HARDWARE												
10/100/1000 Interface	5	7	8	10	8	12	12	12	8	8	8	8
1G SFP Interface	-	-	-	-	-	4	4	4	8	8	8	8
10G SFP+ Interface	-	-	-	-	-	2	2	2	4	4	4	4
Size	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	1U	1U	1U
Power										Redundant		
SonicPoints supported (Maximum)	8	16	16	24	32	48	64	96	128	128	128	128

소닉월코리아
서울특별시 강남구 테헤란로 445 본솔빌딩10F
전화 번호 02-3420-9000 | 팩스 번호 02-569-3600
웹 사이트 www.sonicwall.com

SONICWALL™