SONICWALL

SonicWall 캡처 시큐리티 어플라이언스 1000

SonicWall 캡처 시큐리티 어플라이언스(CSa)는 캡처 지능형 위협 방지(ATP) 기능과 함께 클라우드 분석에 파일을 전송해서는 안 되는 규정과 정책 제한이 있는 고객 또는 모든 데이터를 조직 외부로 보내지 않고 내부에 보관하는 것을 선호하는 고객을 위해 사내 배치 시나리오에 대한 샌드박스 멀웨어 분석 기능을 갖추고 있습니다. CSa 1000은 SonicWall 제품으로부터 전송된 의심스러운 파일을 분석하여 고객이 자신의 파일을 관리 및 보호할 수 있도록 하면서 이전에 확인되지 않은 위협을 매우 정확하고 빠르게 탐지할 수 있습니다. 또한 CSa의 REST API 기능은 위협 인텔리전스 팀, 제3자 보안 시스템 및 공개된 API와 통합할 수 있는 소프트웨어 스택에 매우 효과적인 파일 분석 기능의 이점을 제공합니다.

CSa는 평판 기반 확인, 정적 파일 분석 및 동적 분석을 위한 SonicWall의 특허기술인 실시간 딥 메모리 검사(RTDMI) 엔진을 함께 사용하여 가능한 한 가장 짧은 시간 안에 효율적으로 최상의 악성 파일 탐지율을 보여 줍니다. 클라우드로 전송된 캡처 ATP 분석으로 이미 통합된 SonicWall 보안 제품 생태계는 분석이 확인될 때까지 파일을 차단하는 Block Until Verdict 등의 기능을 갖춘 인라인 보안을 실행할 수 있습니다.

SonicWall 제품이 클라우드 캡처 ATP 대신 CSa 시리즈와 연결된 경우에도 동일한 기능이 지원됩니다.

RTDMI

SonicWall의 특허 출원 중인 실시간 딥 메모리 검사(RTDMI) 파일 분석 엔진은 메모리에 있는 응용 프로그램의 행동을 모니터링하여 의심스러운 파일을 분석하는 새로운 방법입니다. RTDMI는 네트워크 및 샌드박스 분석을 피하기 위해 최신 멀웨어에서 사용된 난독화 또는 암호화 기술을 파악해 문서, 실행 파일, 보관 파일 및 기타 여러 파일 형식에 들어 있는 멀웨어 공격을 매우 정확하게 탐지할 수 있습니다.

실시간 보호

평판 및 글로벌 인텔리전스 검사, 정적 분석, RTDMI 기술을 함께 사용하여 SonicWall 제품의 Block Until Verdict와 같은 기술을 실행하기에 충분히 빠르게 결과를 전달합니다. 이러한 기능은 전체 검사가 완료되고 결과를 캡처 ATP 또는 CSa에서 확인할 수 있을 때까지 최종 사용자가 의심스러운 파일을 다운로드할 수 없도록 방지하기 위해 방화벽에 대한 파일 검사 정책을 고려합니다.

장점:

- RTDMI
  메모리 기반 검사
- 평판 확인, 정적 분석, 동적 분석 등 다단계 분석
- 위협 분석을 위한 API 액세스
- 광범위한 파일 유형 지원
- Block Until Verdict 지원
- 높은 보안 효율성
- 보고 및 역할 기반 접근

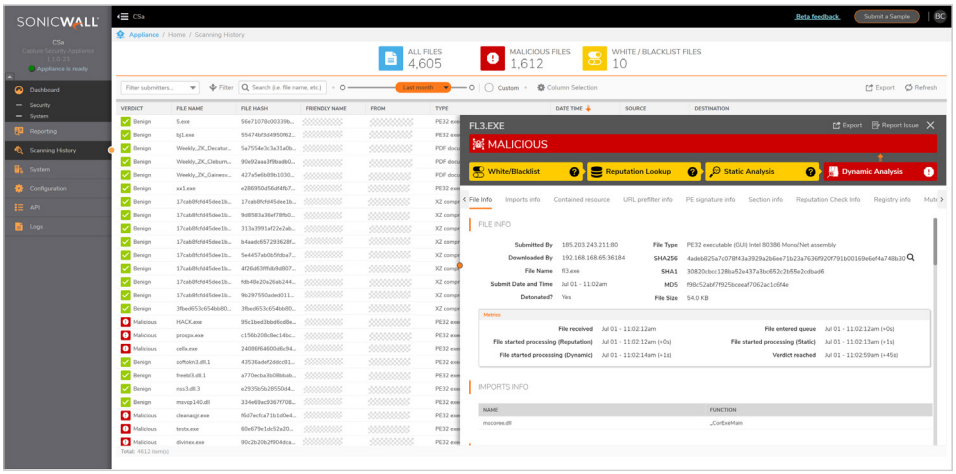
1. *네트워크 연결, 파일 유형, 압축 수준에 따른 분석 처리량은 발표된 수치에 따라 달라질 수 있습니다.*
2. *하드 제한은 없으나 디바이스의 수는 각 디바이스에서 제출한 파일의 수에 따라 결정될 것입니다. 발표 시 권장 범위는 약* 250*개의 디바이스입니다.*
3. SonicOS 6.5.4.6 *버전을 포함한 이후 버전에서 실행할 수 있는 모든* TZ *시리즈,* NSa *시리즈 및* SuperMassive *시리즈에서 지원. SuperMassive* 9800 *및* NSsp 12000 *시리즈에서 지원되지 않음.*

여러 경험을 통한 신뢰와 이점

- CSa는 전 세계 15만 명 이상의 고객이 신뢰하고 사용하는 클라우드 기반 서비스인 SonicWall의 캡처 ATP 기술을 결합한 어플라이언스 폼 팩터입니다.
- CSa는 SonicWall 캡처 ATP 파일 분석을 통해 전 세계적으로 수집된 위협 인텔리전스를 동기화하기 위해 주기적으로 인텔리전스 업데이트 정보를 받습니다.

보고, 분석 및 관리

- CSa는 쉽게 탐색할 수 있는 대시보드와 파일 분석 기록을 사용하여 모든 소스로부터 제출된 파일에 대한 통찰력을 제공합니다. 이를 통해 분석을 위해 제출된 파일에 관한 빈도, 소스, 결과 및 기타 의견을 보여 줍니다.
- 보고 기능은 다양한 역할에 따라 구성된 정기적인 보고서를 예약하는 기능으로 전 세계에 있는 조직의 ATP 보호에 관한 정보를 제공합니다.
- 관리자는 UI에 대한 액세스를 제한할 수 있는 기능과 함께 CSa 1000에 대한 세부적인 액세스를 여러 역할에 제공할 수 있습니다.
- 보안 분석가는 화이트리스트/블랙리스트를 수정하고 디바이스를 허용하고 의심스러운 오탐지(False positive 또는 False negative) 보고할 수 있으며 검사 내역에 액세스할 수 있습니다.
- 네트워크 수준 관리자는 기밀상의 이유로 인해 제출된 파일 및 소스를 확인할 수 없도록 제한을 받을 때도 어플라이언스 운영 설정에 대한 액세스 권한을 받을 수 있습니다.



기능

- 평판 및 글로벌 결과 검색(설정 가능)
- RTDMI 정적 분석 및 동적 분석
- 해시/도메인 화이트리스트/블랙리스트
- 설정 가능한 예약된 보고
- 역할 기반 관리(역할 설정 가능)
- 관리 – 전용 관리 인터페이스 또는 일반 네트워크 인터페이스를 통한 HTTPS 또는 SSH
- SSH 콘솔 액세스
- 기록 및 경보
- 자동 화이트리스트/블랙리스트로 오탐지(False positive 또는 False negative) 보고
- VPN을 통한 직접 연결(IP 주소 지정 가능)
- 폐쇄된 네트워크 운영
- 파일 제출 및 분석을 위한 REST API 지원
- 변조 방지를 위한 보안 부팅 및 신뢰체인을 갖춘 강화된 OS
- 로컬 로깅

1. *네트워크 연결, 파일 유형, 압축 수준에 따른 분석 처리량은 발표된 수치에 따라 달라질 수 있습니다.*
2. *하드 제한은 없으나 디바이스의 수는 각 디바이스에서 제출한 파일의 수에 따라 결정될 것입니다. 발표 시 권장 범위는 약 250개의 디바이스입니다.*
3. SonicOS 6.5.4.6 *버전을 포함한 이후 버전에서 실행할 수 있는 모든 TZ 시리즈, NSa 시리즈 및 SuperMassive 시리즈에서 지원. SuperMassive 9800 및 NSsp 12000 시리즈에서 지원되지 않음.*

배포 옵션

- SonicWall CSa는 빠르고 쉽고 간단하게 배포할 수 있으며 기본 네트워킹 구성,보고 및 장치 액세스를 시작해야합니다.
- CSa는 IP 주소를 지정할 수 있도록 제작되었기 때문에 분석을 위한 파일을 제출하는 디바이스에서 접근할 수 있는 한 어디서든 배포될 수 있습니다.

CSa 1000의 세 가지 주요 배포법:

단일 사무실/단일 장소

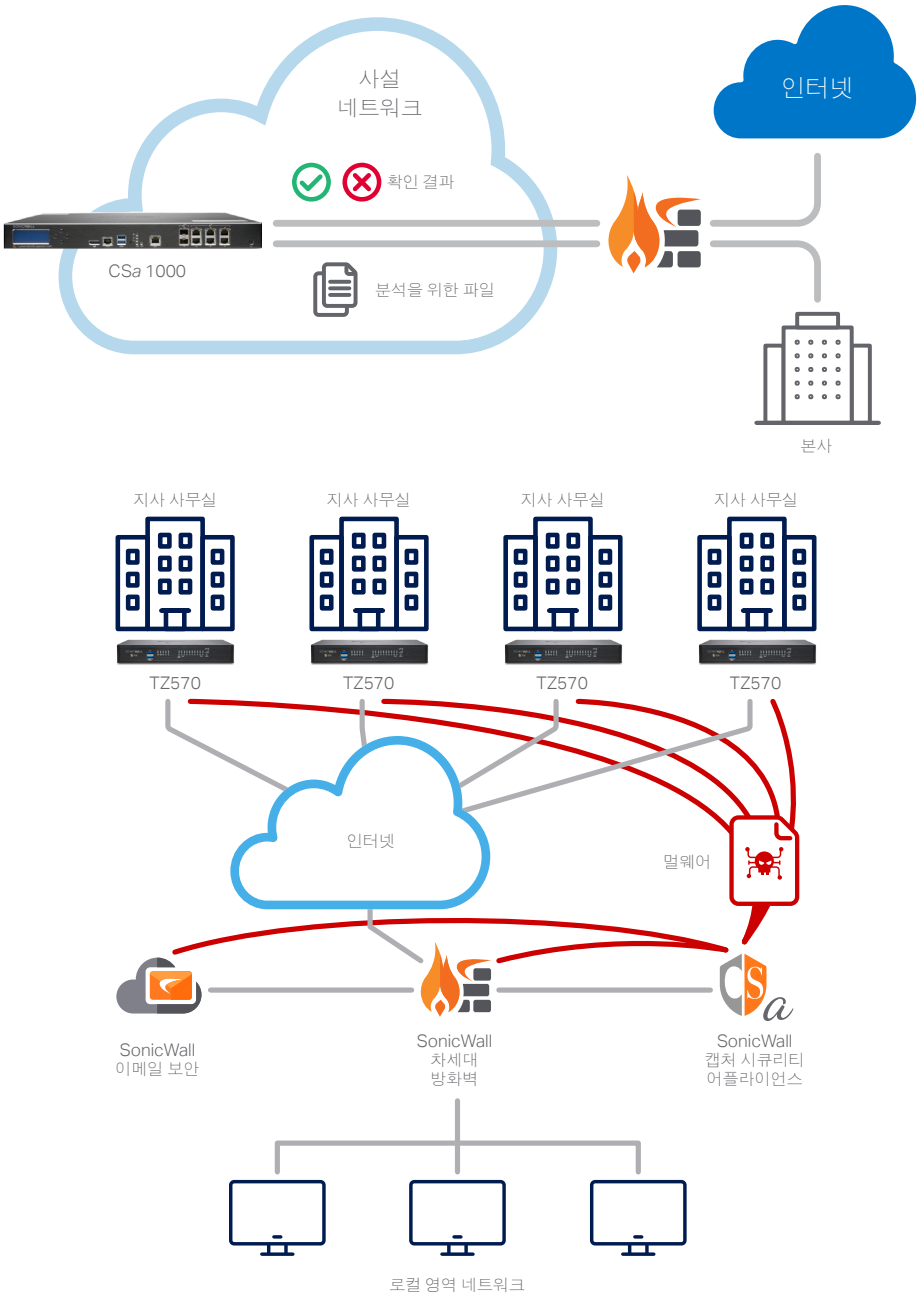
- CSa는 제품에서 IP[1]를 통해 접근할 수 있다면 네트워크 어디에나 배포될 수 있습니다.
- Csa가 배포되면 방화벽과 이메일 시큐리티 시스템(기타 대기 중 솔루션)은 의심스러운 파일을 ATP 분석 클라우드가 아닌 CSa로 다시 보내도록 설정될 수 있습니다.

분산 기업/여러 위치

- 여러 개의 사무실/지사는 단일 CSa 디바이스 액세스를 공유하도록 설정되거나, 중앙 HQ 데이터 센터 또는 모든 디바이스에서 접근할 수 있는 원거리 데이터 센터에 배포될 수 있습니다.
- VPN을 통해 인터넷으로 직접 액세스할 수 있습니다.
- CSa를 지정하기위한 대규모의 SonicWall 시스템 설정은 GMS 또는 빠른 설정과 배포를 위한 클라우드 기반 NSM 중앙 관리 솔루션을 통해 이뤄질 수 있습니다.

REST API 게이트웨이

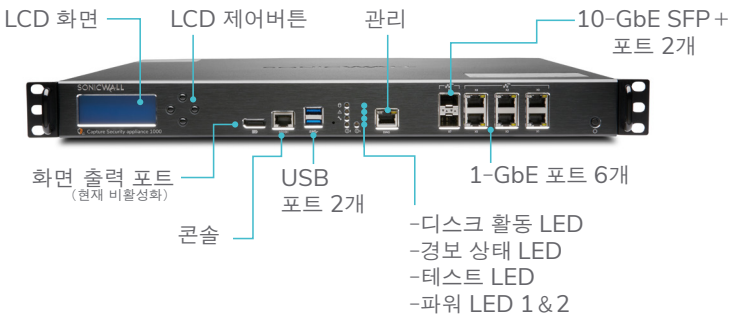
- CSa 시리즈에는 위협 인텔리전스 팀의 스크립트, 웹 포털 통합 및 기타 보안 제품을 통해 분석 및 쿼리 결과 파일을 제출하는 데 사용할 수 있는 REST API 인터페이스가 있습니다.
- CSa의 API 스크립팅 시작법에 관한 설명 및 코드 샘플은 웹 사이트 (https://github.com/sonicwall) 에서 확인할 수 있습니다.

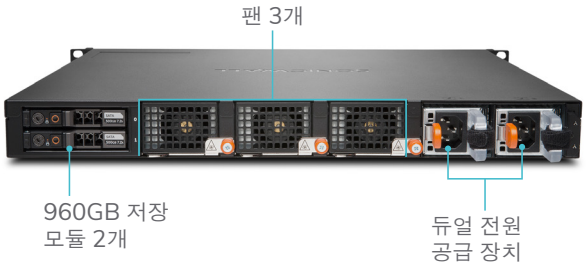


*[1]SonicWall 방화벽은 포트 2259에서 UDP를 통한 액세스가 필요합니다.

1. 네트워크 연결, 파일 유형, 압축 수준에 따른 분석 처리량은 발표된 수치에 따라 달라질 수 있습니다.
2. 하드 제한은 없으나 디바이스의 수는 각 디바이스에서 제출한 파일의 수에 따라 결정될 것입니다. 발표 시 권장 범위는 약 250개의 디바이스입니다.
3. SonicOS 6.5.4.6 버전을 포함한 이후 버전에서 실행할 수 있는 모든 TZ 시리즈, NSa 시리즈 및 SuperMassive 시리즈에서 지원. SuperMassive 9800 및 NSsp 12000 시리즈에서 지원되지 않음.

CSa 1000





SonicWall CSa 1000 사양

기능	
평판 및 글로벌 위협 검색 처리량(시간당 파일)[1]	12,000
실제 파일 믹스 처리량(시간당 파일)[1]	2500
동적 분석(RTDMI) 처리량(시간당 파일)[1]	300
최대 파일 사이즈	100MB
지원되는 최대 디바이스[2]	성능에 따라 다름
최대 아카이브 검사 깊이	3
REST API 지원	예
지원되는 SonicWall 디바이스	TZ, Nsa 및 SuperMassive (SonicOS 6.5.4.6 버전이나 상위 버전에서 실행)[3] 이메일 보안 10.X NSsp 15000 시리즈 - 대기 중 NSv 시리즈(7.X 버전이나 상위 버전) - 대기 중
지원되는 파일 유형	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
데이터 보존 기간	저장에 따라 제한 또는 무제한
저장	1TB SSD(RAID 1) 2개
인터페이스	(6)-포트 1GE, (2)-포트 10Gb SFP+, (2) USB, (1) 콘솔
전용 포트 관리	예(X0)
인증	FIPS 140-2 대기 중
제품 특성	
폼 팩터	1U
치수	17.0 x 16.5 x 1.75in(43 x 41.5 x 4.5cm)
어플라이언스 중량	18.3파운드(8.3kg)
암호화 데이터 가속(AES-NI)	예
MTBF(@ 25° C 또는 77° F) 단위: 시간	129,601
전원	듀얼 전원, 핫스와프 가능
정격 입력	100-240 VAC, 1.79 A
전력 소비	114W
총 열 전달	389 BTU
환경	WEEE, EU RoHS, China RoHS
비 동작 충격	110g, 2msec
배출 가스	FCC, ICES, CE, C-Tick, VCCI; MIC
안전성	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme
작동 시 온도	0° C~40° C(32° F~104° F)
TPM	예

1. 네트워크 연결, 파일 유형, 압축 수준에 따른 분석 처리량은 발표된 수치에 따라 달라질 수 있습니다.
2. 하드 제한은 없으나 디바이스의 수는 각 디바이스에서 제출한 파일의 수에 따라 결정될 것입니다. 발표 시 권장 범위는 약 250개의 디바이스입니다.
3. SonicOS 6.5.4.6 버전을 포함한 이후 버전에서 실행할 수 있는 모든 TZ 시리즈, NSa 시리즈 및 SuperMassive 시리즈에서 지원. SuperMassive 9800 및 NSsp 12000 시리즈에서 지원되지 않음.

제품	SKU
캡처 시큐리티 어플라이언스 CSA 1000	02-SSC-2853
캡처 시큐리티 어플라이언스 CSA 1000과 인텔리전스 업데이트 및 지원 번들 – 1년	02-SSC-5637
캡처 시큐리티 어플라이언스 CSA 1000과 인텔리전스 업데이트 및 지원 번들 – 3년	02-SSC-5638
캡처 시큐리티 어플라이언스 CSA 1000과 인텔리전스 업데이트 및 지원 번들 – 5년	02-SSC-5639

서비스 (CSa 1000 사용에 필요. CSa로 파일을 전송하는 모든 디바이스는 캡처 ATP 라이선스가 반드시 있어야 합니다.)	SKU
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 1년	02-SSC-4712
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 2년	02-SSC-4713
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 3년	02-SSC-4714
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 4년	02-SSC-4715
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 5년	02-SSC-4716
인텔리전스 업데이트, SONICWALL CSA 1000 활성화 및 지원 6년	02-SSC-4717

REST API 활성화 (해당 서비스는 REST API 운영에만 필요합니다. 인텔리전스 업데이트, 활성화 및 지원 서비스와 함께 반드시 적용되어야 합니다.)	SKU
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 1년	02-SSC-4706
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 2년	02-SSC-4707
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 3년	02-SSC-4708
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 4년	02-SSC-4709
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 5년	02-SSC-4710
SONICWALL 캡처 어플라이언스 CSA 1000을 위한 REST API 활성화 6년	02-SSC-4711

1. *네트워크 연결, 파일 유형, 압축 수준에 따른 분석 처리량은 발표된 수치에 따라 달라질 수 있습니다.*
2. *하드 제한은 없으나 디바이스의 수는 각 디바이스에서 제출한 파일의 수에 따라 결정될 것입니다. 발표 시 권장 범위는 약 250개의 디바이스입니다.*
3. SonicOS 6.5.4.6 *버전을 포함한 이후 버전에서 실행할 수 있는 모든* TZ *시리즈,* NSa *시리즈 및* SuperMassive *시리즈에서 지원.* SuperMassive 9800 *및* NSsp 12000 *시리즈에서 지원되지 않음.*

SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 무한한 사이버 보안을 제공합니다. SonicWall은 알려지지 않은 정보를 파악하고 실시간 가시성을 제공하며 혁신적인 경제성을 제공함으로써 전 세계 기업, 정부 및 중소기업의 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 www.sonicwall.com에서 확인할 수 있습니다.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
기타 정보는 웹 사이트에서 확인할 수 있습니다.
www.sonicwall.com

Datasheet-CSa-US-COG-2099