SONICWALL

SonicWall Capture Client

사람보다 빠르게, 자동으로 침해 차단

랜섬웨어 등 각종 맬웨어 기반 공격이 꾸준히 증가하면서, 클라이언트 보호 솔루션의 가치는 엔드포인트 컴플라이언스로만 단편적으로 판단하기 힘들다는 것이 증명되었습니다. 전통적인 안티바이러스 기술이 오랜 기간 발전시켜온 서명 기반 접근법은 신종 맬웨어 및 침입 기술의 발 빠른 진화 속도를 따라잡지 못합니다.

그리고 재택근무, 근무지 자율 선택, BYOD가 널리 확산됨에 따라, 어느 엔드포인트든 일관되게 보호하고, 애플리케이션 취약성을 파악하고, 웹 정책을 강제 적용하는 등의 조치를 단행할 필요성이 커졌습니다. SonicWall Capture Client는 다중 EPP 및 EDR 기능을 갖춘 통합 엔드포인트 제품입니다.

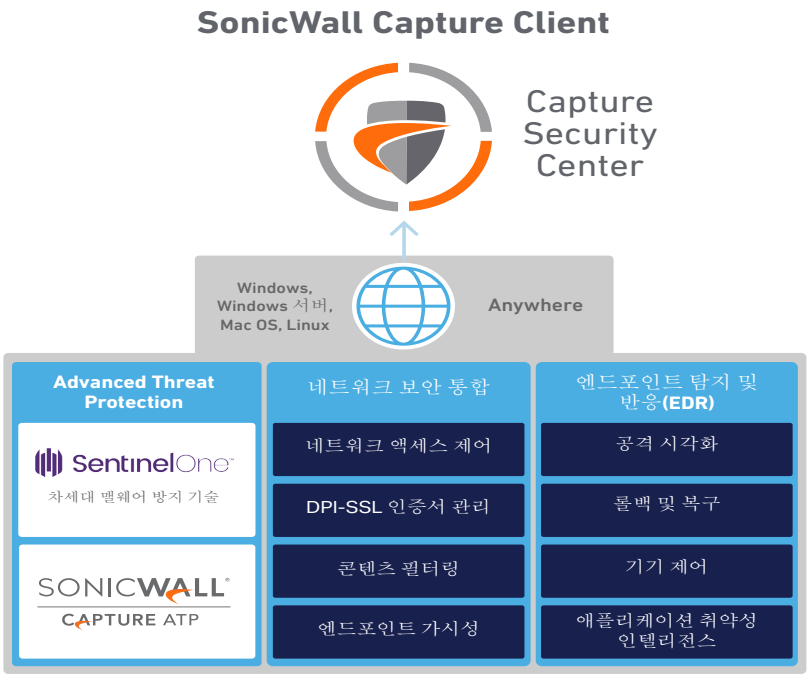
하이라이트

- 조용하게 매우 효과적, 실체적으로 위협 탐지
- 중앙집중식 클라우드 기반 관리, 진정한 멀티 테넌트 기능, 네트워크 및 엔드포인트 보안 강화
- 보안 및 IT 팀의 역량 강화, 사용하기 쉽고 직관적인 인터페이스로 최신 위협 차단

귀사에 적합한 엔드포인트 보안

자료 읽기: sonicwall.com

데이터시트



Capture Client는 NGAV SentinelOne의 행동 기반 고급 위협 보호가 적용되었습니다.

Capture ATP 통합으로 더욱 뛰어난 보안 성능, 더 빠른 응답 시간, 더 낮은 총 소유비용이 특징입니다.

특징 및 이점

지속적인 행동 모니터링

- 파일, 애플리케이션, 프로세스, 네트워크 활동에 대한 완벽한 프로필 제공
- 파일 기반/파일리스 맬웨어로부터 완벽 보호
- 공격을 전방위적으로 모니터링하고 실질적인 인텔리전스 제공

심층적인 가시성으로 위협 탐지

- 행동 지표와 침해 지표(IOC)에 기반한 심층적인 가시성으로 위협 탐지, Windows, MacOS, Linux 기기 모두 보호
- 맞춤 규칙 및 경보로 위협 탐지 및 대응 자동화

Capture Advanced Threat Protection(ATP) 통합

- Windows 기기에 있는 의심스러운 파일을 자동으로 업로드하여 고급 샌드박싱 분석 수행
- 타이머 내장된 맬웨어 등, 잠복된 위협이 실제 실행되기 전에 탐지
- 파일을 클라우드로 직접 업로드할 필요 없이 Capture ATP 파일 판정 데이터베이스를 참조하는 것으로 충분함

고유의 롤백 기능

- 위협을 완전히 제거하는 정책 지원
- 엔드포인트를 악의적인 활동이 개시되기 전의, 확실히 양호한 상태로 자동 복원

다중 레이어 휴리스틱 기반 기술

- 클라우드 인텔리전스, 고급 정적 분석, 동적 행동 보호 활용
- 공격 전후 그리고 공격 중 알려진 맬웨어와 알려지지 않은 맬웨어로부터 보호하고 조치

애플리케이션 취약성 인텔리전스

- 설치된 모든 애플리케이션과 관련된 위험을 카탈로그화
- CVE 세부정보 및 보고된 심각도 수준으로 알려진 취약성 조사
- 이 데이터를 활용하여 패치 우선순위를 정하고 공격 가능 범위 최소화

엔드포인트 네트워크 제어

- 엔드포인트에 방화벽류의 제어 추가
- 추가 검역 룰베이스를 사용하여 감염된 기기 처리

Remote Shell[1]

- 문제 해결, 로컬 구성 변경, 포렌식 조사 수행 시, 기기와 물리적으로 접촉해야 할 필요성 해소

정기 스캔, 주기적 업데이트 불필요

- 사용자의 생산성 저해 없이 항상 최상의 보호를 제공
- 설치 시 전체 스캔, 이후에는 지속적으로 의심스러운 활동 모니터링

SonicWall 방화벽 통합 옵션

- 엔드포인트에서 암호화된 트래픽 심층 패킷 검사(DPI-SSL) 강제 실행 가능
- 신뢰할 수 있는 인증서를 각 엔드포인트에 간편하게 배포
- 보호되고 있지 않은 사용자가 방화벽 보호 없이 인터넷에 액세스하려고 할 때 Capture Client 다운로드 페이지로 이동

콘텐츠 필터링

- 악성 사이트 IP 주소 및 도메인 차단
- 대역폭 한도 설정, 불쾌하거나 비생산적인 웹 콘텐츠 액세스 제한으로 사용자 생산성 향상

기기 제어

- 감염 우려가 있는 기기의 엔드포인트 연결 차단
- 세분화된 허용 목록 정책 사용

Capture Client 기능

기능	Advanced	Premier
클라우드 관리, 보고 및 분석(CSC)	✔	✔
네트워크 보안 통합		
엔드포인트 가시성 및 강제 시행	✔	✔
DPI-SSL 인증서 배포	✔	✔
콘텐츠 필터링	✔	✔
고급 엔드포인트 보호		
차세대 안티맬웨어	✔	✔
Capture Advanced Threat Protection 샌드박싱	✔	✔
ActiveEDR(엔드포인트 탐지 및 대응)		
공격 시각화	✔	✔
롤백 및 복구	✔	✔
기기 제어	✔	✔
애플리케이션 취약성 및 인텔리전스	✔	✔
로그(Rogue)		✔
엔드포인트 네트워크 제어		✔
ActiveEDR 위협 탐지 및 인텔리전스		
심층적인 가시성으로 위협 탐지		✔
Remote Shell[1]		✔
제외 카탈로그		✔

[1] Remote Shell은 S1 콘솔에서 바로, (2FA가 활성화된) 새 계정에서 온디맨드로 사용 가능하도록 출시 예정입니다.

[Capture Client - 시스템 요건 | SonicWall]

MSSP 및 분산 기업의 글로벌 엔드포인트 보안 모범 사례

솔루션 자료 읽기: www.sonicwall.com

SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 경계 없는 사이버 보안(Boundless Cybersecurity) 서비스를 제공합니다. SonicWall은 알려지지 않은 정보에 대한 실시간 가시성을 제공하며 혁신적인 경제성으로 전 세계 기업, 정부, 중소기업 간 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 www.sonicwall.com을 방문하십시오.

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