SONICWALL

SonicWall Capture Client

랜섬웨어 및 기타 악성 맬웨어 기반 공격의 위협이 증가함에 따라 클라이언트 보호 솔루션을 엔드포인트 컴플라이언스에만 기반하여 측정할 수 없다는 것이 입증되었습니다. 전통적인 안티바이러스 기술은 새로 등장하는 맬웨어와 회피 기술의 속도에 맞지 않는 오랜 문제점을 가지고 있는 시그니처 기반 접근법을 사용합니다. 또한, 재택근무, 이동성 및 BYOD가 급증함에 따라, 어디에서나 일관되게 엔드포인트를 보호해야 하는 필요가 커졌습니다.

SonicWall Capture Client는 다중 보호 기능을 갖춘 통합 엔드포인트 제품입니다. SentinelOne이 지원하는 차세대 맬웨어 보호 엔진으로, Capture Client는 기계 학습, 네트워크 샌드박스 통합, 시스템 롤백과 같은 고급 위협 보호 기술을 적용합니다. Capture Client는 또한 신뢰할 수 있는 TLS 인증서를 설치 및 관리함으로써 SonicWall 방화벽의 암호화된 TLS 트래픽(DPI-SSL)의 정밀 검사를 검사도 활용합니다.

Capture Client는 SonicWall Global VPN Client와 공존하며 모든 제품에 대한 정책을 단일 클라우드 기반 관리 콘솔에서 관리할 수 있습니다. Capture Client는 Microsoft Active Directory 그룹 정책이나 기타 타사 소프트웨어 배포 기술을 통하거나, 추가적인 개입 없이 클라이언트가 다운로드하고 쉽게 자가 설치할 수 있는 사용자 정의 된 URL의 제공을 통해 클라이언트에 쉽게 추가할 수 있습니다. 또한, SonicWall 방화벽과 통합 된 경우, Capture Client는 선택적 실행 기능으로 보호되지 않은 클라이언트에 제로터치 배포 환경을 제공합니다.

기능 및 혜택

엔드포인트의 **지속적인 행동 모니터링**은 파일 활동, 응용 프로그램 및 프로세스 활동 및 네트워크 활동에 대한 완전한 프로파일을 작성하는 데 도움이됩니다. 이로 인해 파일 기반 및 파일리스 맬웨어를 막고 조사와 관련된 실행 가능한 인텔리전스와 함께 360도 공격 가시성을 제공할 수 있습니다.

보호를 위한 **다중 계층, 휴리스틱 기반 기술**에는 클라우드 인텔리전스, 고급 정적 분석 및 동적 행동 보호가 포함됩니다. 이는 알려지거나 알려지지 않은 맬웨어를 막고 치료하는데 도움이 됩니다.

정기 스캔 또는 정기 업데이트가 필요하지 않기 때문에 사용자의 생산성을 저해하지 않으면서 항상 최고 수준의 보호를 가능하게 합니다. Capture Client는 설치 시 전체 스캔을 실시하고 이후 지속적으로 의심스러운 활동을 모니터링합니다.

Capture Advanced Threat Protection (ATP) 통합은 고급 샌드박싱 분석을 위하여 엔드포인트가 수행할 수 없는 코드 조작을 통해 의심스러운 파일을 자동으로 업로드합니다. 내장된 타이밍 지연이 있는 맬웨어 등을 실행하기 전에 추가 위협을 중단하십시오. 관리자는 또한 분석을 위해 클라우드에 파일을 업로드할 필요 없이 Capture ATP의 파일 판결 데이터베이스를 참조할 수 있습니다.

독특한 롤백 기능은 또한 위협을 완전히 제거할 뿐만 아니라 목표 고객을 맬웨어 활동이 시작되기 전 상태로 복원하는 정책을 지원합니다. 이로 인해 Windows에서의 랜섬웨어 및 유사한 공격이 있었다고 해도 수동으로 복구하지 않아도 됩니다.

장점

- 독립적인 클라우드 기반 관리
- SonicWall 방화벽과의 시너지 효과
- 보안 정책 시행
- DPI-SSL 인증서 관리
- 지속적인 행동 모니터링
- 기계 학습을 통한 매우 정확한 판단
- 다층 휴리스틱 기반 기술
- 응용 프로그램 취약성 인텔리전스
- 고유한 롤백 기능
- 쉬운 화이트/블랙리스팅
- 자동 맬웨어 분석을 위한 고급 위협 보호 (ATP) 클라우드 샌드박스 캡처
- 수동 파일 검사를 위한 업로드 없이 위협 인텔리전스 공유
- 콘텐츠 필터링
- 장 제어치

응용 프로그램 취약성 인텔리전스는 관리자에게 각 보호된 엔드포인트의 모든 응용 프로그램과 그와 관련된 모든 위험을 분류할 수 있는 능력을 제공합니다. 위험은 해당 버전에 대해보고 된 CVE 및 심각도 수준에 대한 세부 정보가있는 알려진 취약점의 존재를 기반으로, 관리자가 패치의 우선순위를 정하고 공격 영역을 줄이기 위해 실행 가능한 인텔리전스를 제공받을 수 있습니다.

SonicWall 6세대 이상 방화벽을 통한 선택적 통합은 제로 터치 배포와 향상된 엔드포인트 컴플라이언스를 제공합니다. 또한 각 엔드포인트에 신뢰된 인증서를 배포함으로써 암호화된 트래픽 (DPI-SSL)의 심층 패킷 검사를 시행할 수 있습니다.

콘텐츠 필터링으로 조직은 악성 사이트 IP 주소와 도메인을 차단할 수 있으며 대역폭을 제한하거나 불쾌감을 주거나 비생산적인 웹 콘텐츠에 대한 접근을 제한함으로써 사용자의 생산성을 증가시킬 수 있습니다.

장치 제어를 통해 조직은 세분화된 화이트리스팅 정책으로 잠재적으로 감염될 수 있는 장치가 엔드포인트로 연결하는 것을 차단할 수 있습니다.

중앙 집중식 관리 및 고객 보호 레포팅 SonicWall 클라우드 기반 관리 콘솔은 차세대 맬웨어 방지, DPI-SSL 인증서 관리 및 콘텐츠 필터링을 포함한 모든 클라이언트 정책을 단일창으로 관리하는 기능을 합니다.

이 관리 콘솔은 추가 비용 없이 제공되는 멀티테넌트 클라우드 기반 플랫폼입니다. 이 콘솔은 클라이언트 보호 레포팅 및 정책 관리를 제공하며, Microsoft Active Directory 속성에 기반한 정책을 할당할 수 있는 기능을 포함하여 세분화 된 접근 제어 정책을 지원합니다. 이를 통해 관리 서비스 제공자(MSP)는 여러 고객의 클라이언트를 관리하고 레포팅할 수 있습니다. 동시에, 각 고객은 자신의 클라이언트에서만 관리 및 레포팅을 할 수 있습니다.

또한 이 관리 콘솔은 탐지된 맬웨어 위협의 근본 원인을 파악하는 데 도움을 주는 조사 플랫폼으로서 기능하며, 이러한 위협이 재발하는 것을 방지하는 방법에 대해 실행 가능한 인텔리전스를 제공합니다. 예를 들어, 관리자는 클라이언트에서 어떤 응용 프로그램이 실행되고 있는지 쉽게 볼 수 있습니다. 그로 인해 작동되고 있는 취약하거나 또는 승인받지 않은 소프트웨어를 식별할 수 있습니다.

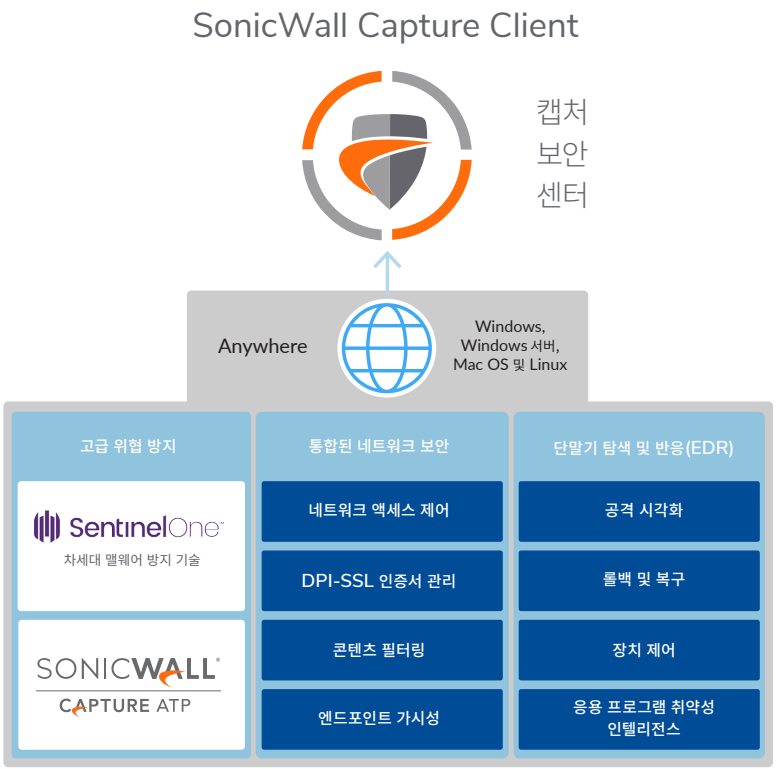
제품 및 플랫폼 지원

SonicWall Capture Client는 다음과 같은 두 가지 제품으로 이용할 수 있습니다.

SonicWall Capture Client Basic은 DPI-SSL 지원 기능과 함께 SonicWall의 모든 차세대 맬웨어 방지 기능과 교정 기능을 제공합니다.

SonicWall Capture Client Advanced은 고급, 추가 고급 롤백 기능, 캡처 ATP 통합, 공격 시각화, 애플리케이션 취약성 인텔리전스 및 콘텐츠 필터링에 대해 위에 나열된 모든 사항을 제공합니다.

두 제품 모두 Windows 7 이상 및 Mac OSX에서 사용할 수 있습니다.



기능 비교		
기능	기본	고급
클라우드 관리, 보고 및 분석(CSC)	✓	✓
통합된 네트워크 보안		
엔드포인트 가시성	✓	✓
DPI-SSL 인증서 배포	✓	✓
콘텐츠 필터링	–	✓
고급 위협 방지		
차세대 안티맬웨어	✓	✓
고급 위협 방지 샌드박싱 캡처	–	✓
엔드포인트 탐색 및 대응		
공격 시각화	–	✓
롤백 및 복구	–	✓
장치 제어	–	✓
응용 프로그램 취약성 및 인텔리전스	–	✓

시스템 요건
운영 시스템
Windows 7 이상
Windows 서버 2008 R2 이상
Mac OS/OSX 10.10 이상
하드웨어
1 GHz 듀얼코어 CPU 이상
OS가 요구하는 경우 1GB RAM 이상(2GB 권장)
디스크 여유 공간 2GB

CAPTURE CLIENT SKU		
제품	유효성	SKU
고급		
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 5-24 단말기	3YR	02-SSC-1518
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 5-24 단말기	1YR	02-SSC-1519
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 25-49 단말기	3YR	02-SSC-1520
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 25-49 단말기	1YR	02-SSC-1521
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 50-99 단말기	3YR	02-SSC-1522
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 50-99 단말기	1YR	02-SSC-1523
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 100-249 단말기	3YR	02-SSC-1524
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 100-249 단말기	1YR	02-SSC-1525
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 250-499 엔드포인트	3YR	02-SSC-1454
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 250-499 엔드포인트	1YR	02-SSC-1455
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 500-999 단말기	3YR	02-SSC-1456
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 500-999 단말기	1YR	02-SSC-1457
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 1000-4999 단말기	3YR	02-SSC-1458
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 1000-4999 단말기	1YR	02-SSC-1459
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 5000-9999 단말기	3YR	02-SSC-1460
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 5000-9999 단말기	1YR	02-SSC-1461
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 10000 이상 단말기	3YR	02-SSC-1462
연중무휴 지원 SONICWALL CAPTURE CLIENT 고급 10000 이상 엔드포인트	1YR	02-SSC-1463
기본		
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 5-24 엔드포인트	3YR	02-SSC-1510
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 5-24 엔드포인트	1YR	02-SSC-1511
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 25-49 단말기	3YR	02-SSC-1512
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 25-49 단말기	1YR	02-SSC-1513
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 50-99 엔드포인트	3YR	02-SSC-1514
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 50-99 엔드포인트	1YR	02-SSC-1515
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 100-249 단말기	3YR	02-SSC-1516
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 100-249 단말기	1YR	02-SSC-1517
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 250-499 단말기	3YR	02-SSC-1444
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 250-499 단말기	1YR	02-SSC-1445
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 500-999 단말기	3YR	02-SSC-1446
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 500-999 단말기	1YR	02-SSC-1447
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 1000-4999 단말기	3YR	02-SSC-1448
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 1000-4999 단말기	1YR	02-SSC-1449
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 5000-9999 단말기	3YR	02-SSC-1450
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 5000-9999 단말기	1YR	02-SSC-1451
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 10000 이상 단말기	3YR	02-SSC-1452
연중무휴 지원 SONICWALL CAPTURE CLIENT 기본 10000 이상 단말기	1YR	02-SSC-1453

SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 Boundless Cybersecurity를 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 다음 웹 사이트를 방문하십시오 www.sonicwall.com.

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

Datasheet-CaptureClient-US-VG-2139