

하나의 창에서 모든 기능을 제어합니다

인식 능력을 높이고, 총체적 보안 관리를 위한 통합 솔루션

사용이 간편한 SONICWALL CAPTURE SECURITY CENTER

SSO(Single-Sign-On)와 단일창(SPOG) 아키텍처를 사용합니다. 확장 가능한 관리 솔루션으로 전체 보안 생태계를 보호하세요.

Capture Security Center(CSC)는 단일 인터페이스에서 종합적인 관리에 필요한 모든 기능을 제공하며, 네트워크, 무선, 이메일, 엔드포인트, 클라우드 보안, 위험 측정기, 자산 관리 등을 위한 분석과 보고를 포함한 모든 기능을 수행합니다.

CSC는 SaaS 솔루션으로서 전체 SonicWall 보안생태계를 360° 감시하는 기민성을 지니고 있습니다. 또한 SPOG 인터페이스를 통해 더 나은 효율성과 운영 융통성을 위해 기능적 통합이 가능합니다.

따라서 장소에 구애받지 않고 모든 웹 기반 기기에서 상세 보고 및 분석을 통해 모든 위협에 신속하게 실시간으로 대응할 수 있습니다.

CSC의 설계는 Security Operation Centers(SOC)의 서비스 레벨 요건을 준수하여 광범위한 사이버 방어 전략을 지원하기 때문에 하나의 웹 기반 앱에서 통합된 보안 관리, 준법 및 기타 위험 관리 전략을 실행할 수 있습니다.



Capture Security Center는 총체적이고 통합된 관리 솔루션을 제공하는 SPOG 애플리케이션입니다. 또한 대부분의 SonicWall 방화벽과 클라우드 서비스에 포함되어 있습니다.

CAPTURE SECURITY CENTER

네트워크, 무선, 스위치, 엔드포인트, 이메일, 클라우드 보안 등을 위해 클라우드가 제공하는 통합된 관리, 보고 및 분석

다 자세히 알아보기

더 나은 효율성과 운영 융통성을 제공합니다

효율성을 높이고, 적은 노력으로 더 빠르고 지능적으로 업무를 해결합니다.

효율성이 높은 CAPTURE SECURITY CENTER

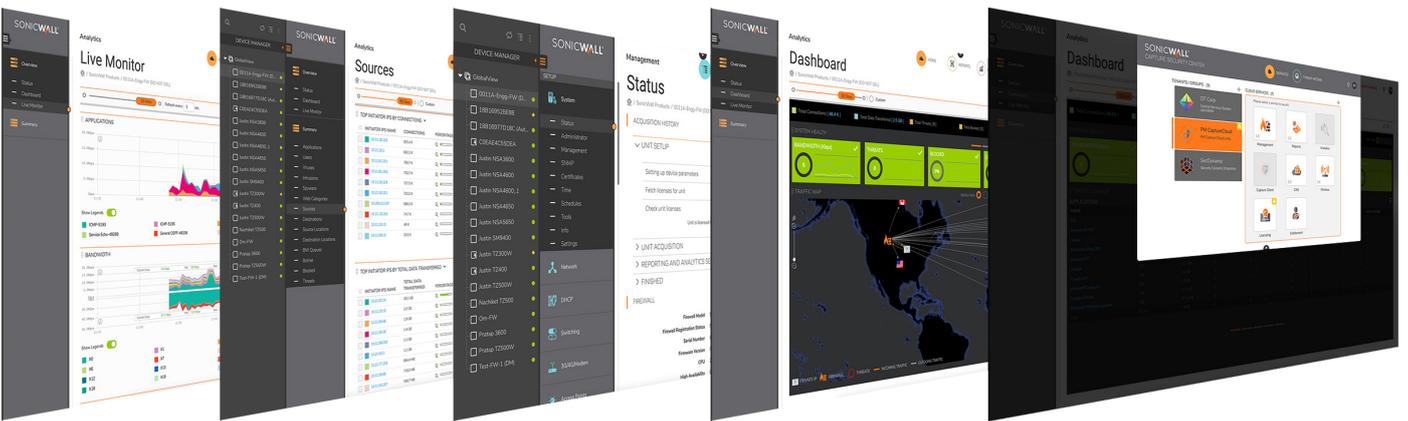
SPOG로 더 많은 기기를 관리하세요. 아카텍처, 사이버 위협, 준법 문제 등을 포함한 보안 인프라와 네트워크의 모든 문제를 해결할 수 있습니다.

CSC는 확장성과 더 나은 관리 조정 기능이 포함된 생산성 관리 도구입니다.

SSO는 클라우드 보안에서 엔드포인트까지 네트워크의 모든 운영 기능을 열 수 있습니다. 클라우드 네이티브 설계로 단순하고 일반적인 프레임워크에서 필요한 모든 기능을 사용할 수 있습니다. 모든 작업이 수월하고 더 효율적입니다.

일상적 업무 수행의 시간과 비용을 줄이세요. 불필요한 보안 사일로를 제거하면 모든 중요한 워크플로에서 "간편한" 효율성을 경험할 수 있습니다. 새로운 기능이 나오면 즉시 활용해 보세요.

전체 SonicWall 보안 스택을 한 장소에서 관리하고, 위험 측정기와 정확한 분석으로 보안 허점과 위협을 파악할 수 있습니다. 또한 시간을 다루는 위협 정보와 상황별 통찰력으로 더 빨리 대응할 수 있습니다. 제로 터치 구축(Zero-Touch Deployment)을 이용하면 지점에서 관리 워크플로를 간소화하고, 잘못된 구성과 인적 오류를 줄이며, 원격 방화벽, 스위치, 액세스 포인트를 간편하게 제공할 수 있습니다.



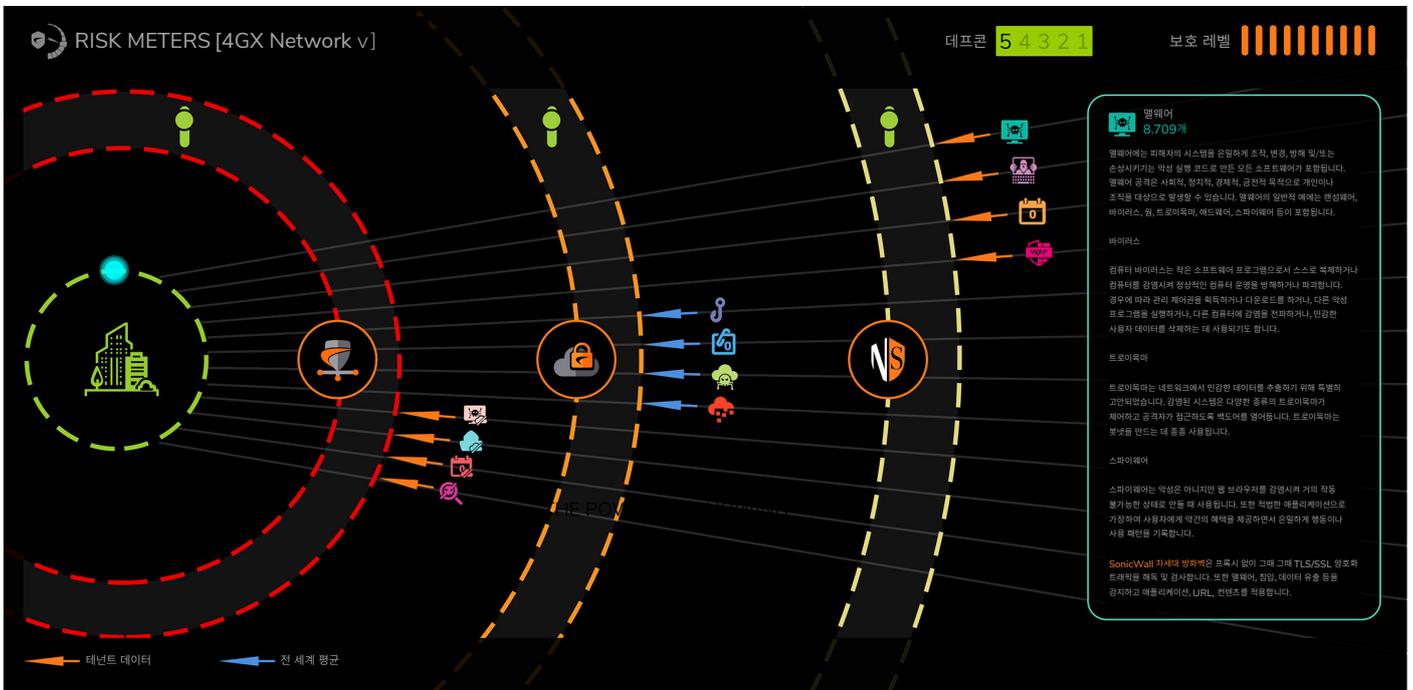
클라우드 네이티브 설계는 효율성과 운영 융통성을 높여줍니다. 하나의 앱에서 보안 사일로를 줄이고 전체 보안 환경의 생산성을 높이세요.

전체 네트워크를 위해 동기화된 사이버 위협 인텔리전스

안전을 확보하세요. 실제 데이터로 실시간 위협과 위험을 파악하세요.

위협을 신속하게 파악하는 CAPTURE SECURITY CENTER

보안 자산의 현재 상태를 바탕으로 맞춤화된 데이터를 최신 사이버 위협 정보와 통합합니다. 실제 위협 데이터를 바탕으로 실시간으로 네트워크를 보호하세요.



위험 측정기는 현재 보호 레벨과 비교한 실시간 위협 데이터를 바탕으로 위험 데이터와 위험 점수를 자동으로 표시합니다. 또한 방어 계층의 허점을 찾아내어 실시간 보안 결정을 합니다. 논리 평가를 바탕으로 보안 기획, 정책 및 예산 수립 결정의 지침을 제공합니다.

SonicWall 위험 측정기를 통해 사용자 네트워크 인프라의 특정 요건을 바탕으로 보안 평가를 맞춤화할 수 있습니다. 네트워크가 직면한 위협을 실시간으로 그래픽 지원 분석을 통해 확인하십시오. 이 내장형 리소스는 보안팀이 위협의 동력을 파악하고 네트워크를 보호하기

위해 해야 할 일을 찾도록 돕습니다. 웹, 클라우드, 애플리케이션, 엔드포인트, 모바일 기기, 데이터베이스, IoT 등에 존재하는 네트워크 위협을 감시하십시오. 잠재적 보안 허점을 가시화하고, 유입되는 공격을 인식하며, 제3자 서비스를 포함한 모든 소스를 모니터링하고, 방어 조치를

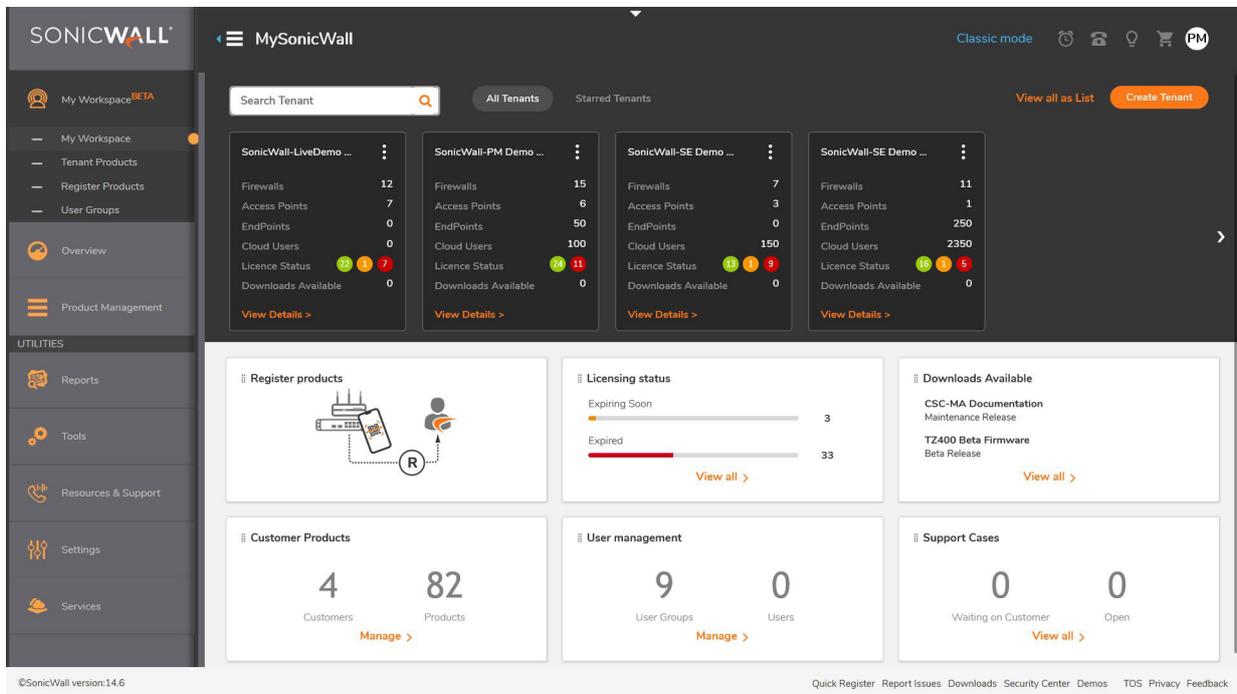
하십시오. 예측 불가능한 공격을 제거하고 실시간으로 발생하는 일을 바탕으로 네트워크 보안을 강화하십시오.

중단이나 부하를 주지 않는 보안 관리

뛰어난 제어력. 보안 업무를 한 장소에서 해결하세요.

완전한 CAPTURE SECURITY CENTER

보안 환경을 한꺼번에 볼 수 있는 강력한 기능으로 관리와 계정 프로세스를 간소화하고, 의사결정을 가속화하며, 지원을 개선하고, 보안 허점을 수정합니다.



Capture Security Center 클라우드 콘솔에서 접근 가능한 MySonicWall의 My Workspace에서 복잡한 보안 작업을 간단하고 더 효율적인 방법으로 실행할 수 있습니다. 또한 체계적인 작업흐름으로 모든 캠퍼스, 지점 또는 직무 그룹에 있는 여러 테넌트를 간편하고 신속하게 온보딩, 설정, 관리하고, 대량 제품 등록을 실시하고, 라이선스 및 지원을 활성화하며, 주문형 제품 체험을 개시할 수 있도록 합니다.

테넌트 워크플로를 통해 Capture Security Center에서 관리되는 제품에 대해 역할 기반의 세부적 컨트롤뿐만 아니라 조직 전반에서 보안 운영 팀에 즉시 접근할 수 있습니다. 직관적 대시보드를 통해 사용자는 라이선스가 만료된 제품이나 소프트웨어/펌웨어 업데이트가 필요한 제품을 즉시 확인하고 인식할 수 있습니다. 내장형 셀프 서비스 포털에서 테넌트와 연결하고, 협업하며, 의사소통할 수 있을 뿐만 아니라, 문제를

파악하고, 추적하며, 해결하고, 지원을 받을 수 있습니다.

CSC 기능 요약

관리

- 대부분의 기능에 SPOG 액세스
- 다중 동시 사용자 세션
- 중앙 집중식 보안 및 네트워크 관리
- 범용 대시보드
- 방화벽 관리
- SonicWall Switch Management
- 무선 관리
- 연합 정책 구성
- 그룹 레벨에서 정책 정의
- 기기에서 단일 기기 또는 그룹 기기로 정책 복사
- 주문 관리 및 워크플로 변경
- 제로 터치 구축(Zero-Touch Deployment)
- 제로 터치 사전 제공 기기 구성
- VPN 배치 및 구성
- 적극적인 기기 모니터링 및 경고
- 애플리케이션 가시화 및 정보
- API, CLI 및 SNMP 지원
- Capture Client 관리
- 클라우드 앱 보안 관리
- 호스팅 이메일 보안 관리
- MySonicWall과 My Workspace

- 위험 측정장치
- Security Center
- Cloud App Security – 새도우 IT
- 라이선스 관리
- 역할 기반 관리(사용자, 그룹)
- 방화벽 어플라이언스를 위한 환경 설정 파일 백업

모니터링

- 기기 모니터링 및 경고
- 실시간 IPFIX 데이터 흐름
- 적극적인 기기 모니터링 및 경고
- SNMP 릴레이 관리
- VPN 및 방화벽 상태 모니터링
- 위험 측정장치

보고

- 중앙 집중식 방화벽 로깅
- Syslog 또는 IPFIX 기반 보고서
- 맞춤형 예약 PDF 보고서
- 다중 위협 보고서
- 사용자 중심의 보고서
- 애플리케이션 사용 보고서
- 봇넷 보고서
- Geo IP 보고서
- MAC 주소 보고서

- Capture ATP 보고서
- 불법 무선 액세스 포인트 보고서
- Cloud App Security(CAS) 보고서
- Capture Client 보고서
- 인터페이스당 광대역 및 서비스 보고서

분석

- 사용자 기반 활동
- 애플리케이션 사용
- Capture Client를 사용한 외적 가시성
- 실시간 역동적 가시화
- 드릴 다운 및 피벗 기능

라이선싱 및 패키징

클라우드 기반 서비스는 다음의 패키지 옵션으로 제공 가능합니다.

1. CSC Basic Management (Lite)

이 버전은 방화벽 시스템, 환경 설정 및 펌웨어 업그레이드의 백업/복원에 가장 적합합니다. AGSS 또는 CGSS 구독을 포함하는 모든 방화벽은 방화벽을 관리하는 것을 돕기 위해 이러한 기본 관리 기능을 활성화할 수 있습니다.

2. CSC Management

이 유료 구독 옵션은 워크플로 자동화와 제로 터치 구축 기능을 포함하여 완전한 관리 기능을 활성화합니다.

3. CSC Management and Reporting

이 라이선스 옵션은 그룹 레벨이나 테넌트 기반 관리를 받으며 지리적으로 분산된 장소에 다수의 방화벽이 배치되기 때문에 대형 기관에게 이상적입니다. 여기에는 미드 마켓 조직, 분산된 기업, 공공 부문, 교육구와 캠퍼스가 많은 교육 기관, 관리형 서비스 제공업체(MSP) 등이 포함됩니다.

이 구독 옵션은 완전한 관리 기능 이외에도 정기적으로 또는 주문형으로 보안 및 네트워크 성능 검토 및 감사를 하도록 완전한 보고 기능을 제공합니다. 이러한 기능은 라이브 채팅 및 테이블을 사용하는 온스크린 대화식 범용 대시보드를 사용하거나 예약된 내보내기 보고서를 통한 오프스크린을 사용하여 실행할 수 있습니다.

4. CSC Analytics

모든 Capture Security Center 구독 옵션에게 효과적인 애드온 서비스입니다. 서비스를 활성화하면 SonicWall Analytics와 SonicWall Cloud App Security 도구 및 서비스에 대한 완전한 액세스를 제공하여 포괄적인 드릴다운 및 피벗 기능을 통해 네트워크 포렌식 및 위협 포착을 실시합니다. CSC Analytics에는 또한 30일 연장 로그 보관 및 365일 보고가 포함되어 있습니다.

지원되는 방화벽 모델

Capture Security Center는 SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSA Series, NSa 2650-6650 및 NSv Series 방화벽을 사용하는 고객이 이용할 수 있습니다. SuperMassive 9000 Series, NSa Series 및 NSsp 12400 – 12800의 경우 CSC 관리 구독 옵션은 해당 AGSS 구독 활성화의 일부로서 자동으로 활성화됩니다.

CAPTURE SECURITY CENTER

	Management	Reporting ⁴	Analytics ⁴
Entry-level FW	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100
Mid-range FW	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400
High-end FW	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600

⁴High-end FW를 위한 보고 및 분석 지원은 On_prem Analytics에서만 이용 가능합니다.

기능		CSC Management Lite	CSC Management	CSC Management and Reporting	SaaS Analytics	On Premises Analytics
관리	백업/복원 - 방화벽 시스템	예	예	예	예	예 ²
	백업/복원 - 방화벽 환경 설정	예	예	예	예	예 ²
	펌웨어 업그레이드	로컬 파일에서만	로컬 파일에서 또는 MySonicWall 에서	예	로컬 파일에서만	로컬 파일에서만 ³
	작업 예약	-	예	예	-	-
	그룹 방화벽 관리	-	예	예	-	-
	상속 - 포워드/리버스	-	예	예	-	-
	제로 터치 구축 ¹	-	예	예	-	-
	오프라인 방화벽 서명 다운로드	-	예	예	-	-
	워크플로	-	예	예	-	-
	라이선스 풀 - 검색, 공유, 사용한 활성화 코드 목록	-	예	예	-	-
보고 (Netflow/IPFIX 기반)	보고서 예약, 라이브 모니터, 요약 대시보드	-	-	예	예	예
	보고서 다운로드: 애플리케이션, 위협, CFS, 사용자, 트래픽, 소스/목적지(1년 흐름 보고)	-	-	예	예	예
분석 (Netflow/IPFIX 기반)	드릴다운 및 피벗을 사용한 네트워크 포렌식 및 위협 포착	-	-	-	예	예
	Cloud App Security - 새도우 IT	-	-	-	예	아니요
	데이터 보존	-	-	-	30일 트래픽	1년
기술 지원		웹 케이스만 해당	24x7 지원	24x7 지원	24x7 지원	24x7 지원

¹ 펌웨어 6.5.2+를 사용하는 SOHO-W, TZ, NSA 시리즈 및 펌웨어 6.5.1.1+를 사용하는 NSa 2650-6650 지원. SOHO 또는 NSv 시리즈 미지원.

² AGSS/CGSS 서비스 또는 유료 Capture Security Center 서비스 필수

³ 24x7 지원 라이선스 필수

주문 정보

제품	SKU
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 to 100 1Yr	01-SSC-3664
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 to 100 2Yr	01-SSC-9151
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 to 100 3Yr	01-SSC-9152
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3665
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9214
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9215
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 1Yr	01-SSC-3435
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 2Yr	01-SSC-9148
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 3Yr	01-SSC-9149
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3879
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9154
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9202
SonicWall Capture Security Center Analytics for SOHO-W, SOHO 250, SOHO250W, TZ Series, NSv 10 to 100 1Yr	02-SSC-0171
SonicWall Capture Security Center Analytics for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	02-SSC-0391

인터넷 브라우저

- Microsoft® Internet Explorer 11.0 이상(호환 모드 사용 금지)
- Mozilla Firefox 37.0 이상
- Google Chrome 42.0 이상
- Safari(최신 버전)

Capture Security Center가 관리하며 지원되는 SonicWall 어플라이언스

- SonicWall 네트워크 보안 어플라이언스: SuperMassive E10000 및 9000 Series, E-Class NSA, NSsp Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security(CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access: SMA 100 Series

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 www.sonicwall.com을 방문하십시오.