SONICWALL

SonicWall Capture Client

Stale rosnące zagrożenie ze strony ransomware i innych ataków wykorzystujących złośliwe oprogramowanie sprawia, że skuteczność klienckich rozwiązań ochrony nie może być już mierzona wyłącznie poziomem zgodności ze standardami. Tradycyjne technologie antywirusowe wykorzystują od dawna nieefektywne podejście oparte na sygnaturach, nie nadążając za tempem, w jakim powstaje nowy malware i techniki omijania zabezpieczeń. Co więcej, wraz z rozpowszechnieniem się telepracy, mobilności i modelu BYOD rośnie potrzeba zapewnienia spójnej ochrony i egzekwowania polityk bezpieczeństwa sieciowego dla punktów końcowych znajdujących się w dowolnym miejscu.

SonicWall Capture Client to zunifikowana i wszechstronna oferta z zakresu bezpieczeństwa punktów końcowych. W oparciu o stworzoną przez SentinelOne platformę ochrony przed złośliwym oprogramowaniem nowej generacji rozwiązanie Capture Client wykorzystuje takie zaawansowane techniki, jak uczenie maszynowe, integracja z wielosilnikową piaskownicą (sandboxing) oraz przywracanie systemu. Capture Client stosuje również dogłębną inspekcję zaszyfrowanego ruchu TLS (DPI-SSL) na zaporach SonicWall - poprzez instalowanie i zarządzanie zaufanymi certyfikatami TLS.

Capture Client współdziała z SonicWall Global VPN Client, a zarządzanie politykami dla wszystkich produktów odbywa się z jednej konsoli opartej na chmurze. Rozwiązanie Capture Client można łatwo wdrożyć na dowolnym kliencie dodanym przy użyciu zasad grupy Microsoft Active Directory albo za pomocą dowolnego innego rozwiązania do instalowania oprogramowania. Można także dostarczyć specjalnie przygotowane adresy URL, przy użyciu których użytkownicy urządzeń końcowych pobiorą oraz samodzielnie i bez problemów zainstalują ochronę. Co więcej, gdy Capture Client jest zintegrowany z zaporami SonicWall, możliwe staje się wtedy bezobsługowe wdrażanie rozwiązania na niechronionych klientach, z opcjonalnymi mechanizmami wymuszania.

Scentralizowane zarządzanie i raportowanie ochrony klienta

Oparta na chmurze konsola zarządzania SonicWall oraz globalny pulpit nawigacyjny zostały zaprojektowane tak, aby dostarczać dostawcom zarządzanych usług bezpieczeństwa (MSSP) migawki stanów ochrony ich klientów w całościowym widoku. Administratorzy mogą zobaczyć stan ochrony każdego usługobiorcy, który jest oceniany na podstawie liczby infekcji, występujących luk, wersji zainstalowanego oprogramowania Capture Client oraz najczęściej blokowanych przez mechanizm Content Filtering użytkowników i treści. Pulpit nawigacyjny może również informować, które urządzenia są online i działają.

Dzięki funkcji Global Policy administratorzy mogą stosować tę same bazowe polityki bezpieczeństwa u wszystkich swoich użytkowników, co ułatwia dodawanie kolejnych. Tym sposobem dostawcy usług MSSP mogą szybko wdrażać zabezpieczenia przed nowymi zagrożeniami u wszystkich usługobiorców objętych tymi politykami. Po włączeniu opcji Inheritance u wszystkich nowych usługobiorców zostają zastosowane reguły Global Policy. Gdy jest ona natomiast wyłączona, można tworzyć i modyfikować unikalne zasady dla poszczególnych użytkowników - od filtrowania treści, poprzez ochronę przed złośliwym oprogramowaniem, po zarządzanie certyfikatami DPI-SSL.

Dostępna jest obsługa szczegółowych polityk kontroli dostępu, w tym możliwość przypisywania reguł na podstawie atrybutów Microsoft Active Directory, takich jak grupa użytkowników. Umożliwia to dostawcom MSSP/MSP dostarczanie usług raportowania i zarządzania urządzeniami klienckimi dla wielu usługobiorców. Co istotne, każdy z usługobiorców ma kontrolę i dostęp do raportów dotyczących wyłącznie jego urządzeń klienckich.

Konsola zarządzania działa również jako platforma do czynności dochodzeniowych, ułatwiając identyfikację pierwotnej przyczyny wykrytych zagrożeń malware i dostarczając przydatne informacje o sposobach zapobiegania powtórkom tego rodzaju incydentów. Przykładowo, administrator może łatwo sprawdzić, jakie aplikacje są uruchomione na kliencie. To z kolei może pomóc zidentyfikować komputery, na których działa oprogramowanie, które jest podatne na ataki albo nieautoryzowane.

Korzyści

- Niezależne, oparte na chmurze zarządzanie
- Synergia z zaporami sieciowymi SonicWall
- Wymuszanie polityk bezpieczeństwa
- Zarządzanie certyfikatami DPI-SSL
- Ciągłe monitorowanie behawioralne
- Duża dokładność wykrywania dzięki uczeniu maszynowemu
- Wielowarstwowe techniki oparte na heurystyce
- Analiza luk w zabezpieczeniach aplikacji
- Unikalna funkcja rollback (przywracania poprzedniego stanu systemu)
- Globalny pulpit stanu ochrony wszystkich usługobiorców
- Łatwe tworzenie globalnych polityk
- Łatwe tworzenie list zezwalaj/blokuj
- Capture Advanced Threat Protection (ATP) – oparta na chmurze piaskownica (sandbox) do automatycznej analizy złośliwego oprogramowania
- Nie wymagająca przesyłania danych funkcja threat intelligence do manualnej inspekcji plików
- Filtrowanie treści
- Kontrola urządzenia

Funkcje i korzyści

Ciągłe monitorowanie behawioralne

- Daje wgląd w kompletne profile aktywności plików, aplikacji, procesów oraz sieci
- Chroni zarówno przed malware wykorzystującym pliki, jak i niekorzystającym z nich
- Dostarcza pełen 360-stopniowy obraz ataku oraz gotowe do użycia dane wywiadowcze

Wielowarstwowe techniki oparte na heurystyce

- Wykorzystuje inteligencję z chmury, zaawansowaną analizę statyczną i dynamiczną ochronę behawioralną
- Chroni i neutralizuje skutki działania znanego i nieznanego malware przed, podczas i po ataku

Brak potrzeby regularnego skanowania i okresowych aktualizacji

- Zapewnia najwyższy poziom ochrony w trybie ciągłym bez wpływu na wydajność klienta
- Oferuje pełne skanowanie podczas instalacji, a potem ciągłe monitorowanie pod kątem podejrzanych aktywności

Integracja z Capture Advanced Threat Protection (ATP) (dla urządzeń Windows)

- Automatycznie przesyła podejrzane pliki z urządzeń z systemem Windows w celu zaawansowanej analizy przy użyciu piaskownicy
- Znajduje uśpione zagrożenia przed wykonaniem, takie jak malware z wbudowanym opóźnieniem czasowym
- Wykorzystując referencyjną bazę danych Capture ATP, ocenia pliki bez konieczności przesyłania ich do chmury

Unikalna funkcja rollback (dla Windows)

- Obsługuje polityki, które usuwają zagrożenie całkowicie
- Przywraca punkty końcowe do stanu zanim działanie malware zostało zainicjowane
- Eliminuje potrzebę ręcznego odtwarzania w przypadku ransomware i podobnego typu ataków

Analiza luk w zabezpieczeniach aplikacji (dla Windows i MacOS)

- Kataloguje każdą zainstalowaną aplikację i związane z nią ryzyko
- Bada znane podatności w oparciu o dane CVE i zgłoszone poziomy istotności luk
- Używa tych informacji do ustalania priorytetów łatania i ograniczania powierzchni ataku

Opcjonalna integracja z zaporami SonicWall

- Umożliwia wymuszenie głębokiej inspekcji pakietów w ruchu szyfrowanym (DPI-SSL) na punktach końcowych
- Ułatwia wdrażanie zaufanych certyfikatów na każdym punkcie końcowym
- Przed udzieleniem dostępu do Internetu kieruje niechronionych użytkowników znajdujących się za zaporą sieciową do strony pobierania Capture Client

Filtrowanie treści (dla Windows i MacOS)

- Blokuje adresy IP i domeny złośliwych witryn
- Zwiększa produktywność użytkowników, ograniczając pasmo lub dostęp do niepożądanych treści internetowych

Kontrola urządzeń (dla Windows i MacOS)

- Blokuje potencjalnie zainfekowane urządzenia przed łączeniem się z punktami końcowymi
- Stosuje szczegółowe polityki w oparciu o listy blokuj/zezwalaj

Wersje i wsparcie platformy

Rozwiązanie SonicWall Capture Client jest dostępne w dwóch wersjach:

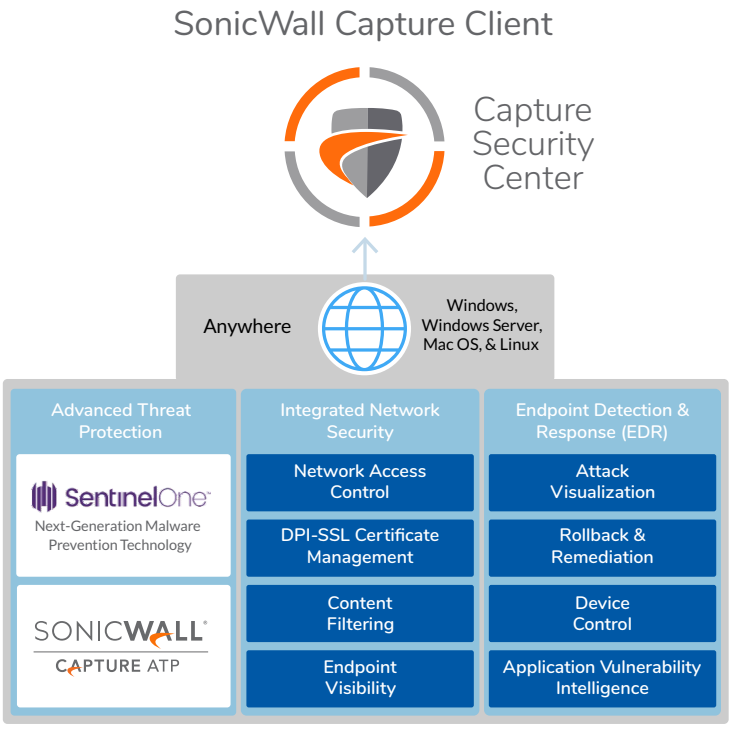
SonicWall Capture Client Basic:

- Pełna ochrona SonicWall przed malware nowej generacji
- Funkcje naprawcze
- Możliwości obsługi DPI-SSL

SonicWall Capture Client Advanced:

- Wszystkie możliwości wersji Basic
- Zaawansowane funkcje rollback
- Integracja Capture ATP
- Wizualizacja ataku
- Analiza luk w zabezpieczeniach aplikacji
- Filtrowanie treści

Obie wersje są dostępne dla systemów Windows 7 i nowszych, Mac OSX i Linux (więcej informacji o wymaganiach systemowych poniżej).



PORÓWNANIE FUNKCJI		
Funkcja	**Basic**	**Advanced**
Cloud Management, Reporting & Analytics (CSC)	✓	✓
Integrated Network Security		
Endpoint Visibility	✓	✓
DPI-SSL Certificate Deployment	✓	✓
Content Filtering	–	✓
Advanced Threat Protection		
Next-Generation Antimalware	✓	✓
Capture Advanced Threat Protection Sandboxing	–	✓
Endpoint Detection and Response		
Attack Visualization	–	✓
Rollback & Remediation	–	✓
Device Control	–	✓
Application Vulnerability and Intelligence	–	✓

WYMAGANIA SYSTEMOWE
Systemy operacyjne
Windows 7 I nowsze
Windows Server 2008 R2 I nowsze
Mac OS/OSX 10.10 I nowsze
Amazon Linux AMI
Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+
Ubuntu 12.04, 14.04, 16.04, 16.10
CentOS 6.5+, 7.0+
Oracle Linux OL (wcześniej znany jako Oracle Enterprise Linux lub OEL) v6.5-6.9 I v7.0+
SUSE Linux Enterprise Server 12
Sprzęt
1 GHz Dual-core CPU lub lepszy
1 GB RAM lub więcej, jeśli wymaga tego OS (zalecane 2 GB)
2 GB wolnego miejsca na dysku

CAPTURE CLIENT - numery SKU		
Produkt	Ważność (lata)	SKU
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS with 24X7 Support	3	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS with 24X7 Support	1	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS with 24X7 Support	3	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS with 24X7 Support	1	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS with 24X7 Support	3	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS with 24X7 Support	1	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS with 24X7 Support	3	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS with 24X7 Support	1	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS with 24X7 Support	3	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS with 24X7 Support	1	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS with 24X7 Support	3	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS with 24X7 Support	1	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS with 24X7 Support	3	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS with 24X7 Support	1	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS with 24X7 Support	3	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS with 24X7 Support	1	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPOINTS with 24X7 Support	3	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPOINTS with 24X7 Support	1	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS with 24X7 Support	3	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS with 24X7 Support	1	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS with 24X7 Support	3	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS with 24X7 Support	1	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS with 24X7 Support	3	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS with 24X7 Support	1	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS with 24X7 Support	3	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS with 24X7 Support	1	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS with 24X7 Support	3	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS with 24X7 Support	1	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS with 24X7 Support	3	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS with 24X7 Support	1	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS with 24X7 Support	3	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS with 24X7 Support	1	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS with 24X7 Support	3	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS with 24X7 Support	1	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS with 24X7 Support	3	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS with 24X7 Support	1	02-SSC-1453

O firmie SonicWall

W erze hiper-rozproszonego środowiska pracy, gdy wszyscy są zdalni, mobilni i niechronieni, SonicWall konsekwentnie wprowadza w życie swoją koncepcję Boundless Cybersecurity. Zapewniając wgląd w czasie rzeczywistym i niezwykle ekonomiczne podejście do ochrony, SonicWall wypełnia luki w zabezpieczeniach w przedsiębiorstwach, instytucjach rządowych oraz małych i średnich firmach na całym świecie. Aby uzyskać więcej informacji, odwiedź stronę www.sonicwall.com oraz śledź nas w serwisach Twitter, LinkedIn, Facebook I Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Więcej informacji na stronie:
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150