SONICWALL

Usługa SonicWall Capture Advanced Threat Protection

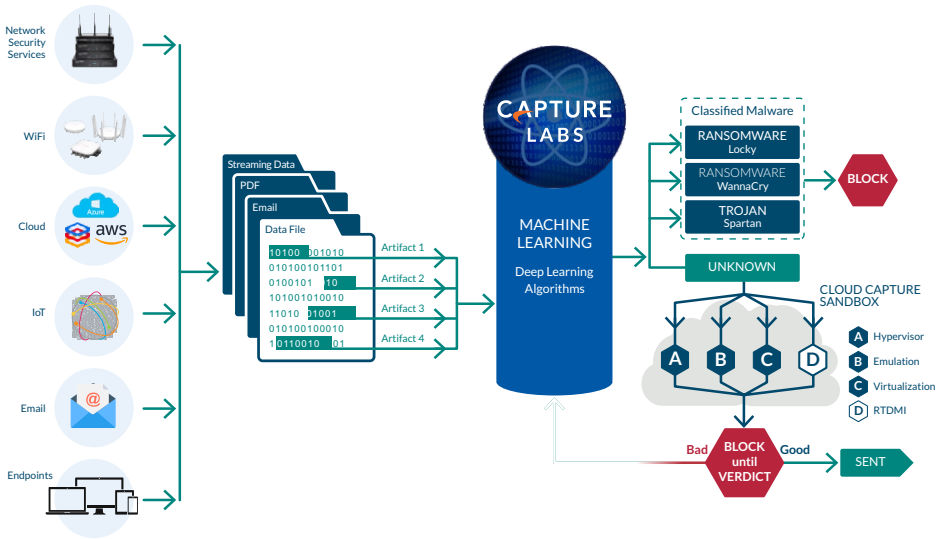
Wykrywanie i blokowanie ataków zero-day oraz innych nieznanych zagrożeń

Aby zapewnić sobie skuteczną ochronę przed zagrożeniami typu zero-day, organizacje potrzebują rozwiązań wykorzystujących technologie analizy złośliwego oprogramowania, umożliwiających wykrywanie omijających zabezpieczenia zaawansowanych ataków oraz malware – teraz i w przyszłości.

Aby chronić firmy przed rosnącym zagrożeniem atakami typu zero-day, SonicWall Capture Advanced Threat Protection (ATP) — oparta na chmurze usługa dostępna z zaporami sieciowymi SonicWall — wykrywa i blokuje potencjalne zaawansowane zagrożenia do momentu uzyskania wyniku analizy. Usługa Capture ATP to jedyna metoda wykrywania zaawansowanych zagrożeń, która łączy wielowarstwowy sandboxing z techniką Real-Time Deep Memory Inspection (RTDMI™), pełną emulacją systemu oraz wirtualizacją w celu analizy zachowania podejrzanego kodu.

Ta niezwykle skuteczna kombinacja wykrywa więcej zagrożeń niż jednosilnikowe rozwiązania typu sandbox, stworzone dla wybranych środowisk obliczeniowych i podatne na techniki omijania zabezpieczeń.

Rozwiązanie skanuje ruch i wyławia podejrzany kod, analizując - w przeciwieństwie do innych rozwiązań typu gateway – szerokie spektrum rozmiarów i typów plików. Globalna infrastruktura threat intelligence szybko wdraża sygnatury dla nowych zidentyfikowanych zagrożeń na wszystkich urządzeniach ochrony sieci SonicWall, zapobiegając w ten sposób dalszej infiltracji. Chronione organizacje korzystają z wysokiego poziomu bezpieczeństwa, szybkiego czasu reakcji i niższego całkowitego kosztu posiadania.



Wielosilnikowe, oparte na chmurze rozwiązanie do blokowania na bramie ataków typu zero-day i innych nieznanych zagrożeń

Korzyści

- Duża skuteczność ochrony przed nieznanymi zagrożeniami
- Wdrażanie sygnatur w czasie zbliżonym do rzeczywistego chroni przed kolejnymi atakami
- Zmniejszony całkowity koszt posiadania
- Blokowanie plików na bramie do momentu uzyskania wyniku analizy
- Wiele silników równolegle przetwarza pliki w celu szybkiego uzyskania wyniku badania
- Mechanizm RTDMI firmy SonicWall blokuje nieznany malware, wykorzystując działające w czasie rzeczywistym i w pamięci operacyjnej techniki inspekcji

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Możliwości

Wielosilnikowa zaawansowana analiza zagrożeń - usługa Capture ATP rozszerza ochronę zapory sieciowej o wykrywanie i zapobieganie zagrożeniom typu zero-day. Firewall bada ruch, wykrywa i blokuje włamania oraz znane malware. Podejrzane pliki są natomiast wysyłane do chmury SonicWall Capture ATP w celu dalszej ich analizy. Wielosilnikowa platforma sandboxingu, która wykorzystuje technologię Real-Time Deep Memory Inspection, zwirtualizowaną piaskownicę (sandbox), pełną emulację systemu oraz analizę na poziomie wirtualizatora, uruchamia podejrzany kod i analizuje jego zachowanie. W rezultacie zapewnia kompleksowy wgląd w złośliwą aktywność, ujawnia techniki omijania zabezpieczeń i maksymalizuje wykrywanie zagrożeń typu zero-day.

Real-Time Deep Memory Inspection (RTDMI) - zgłoszona do opatentowania technologia SonicWall dopełnia opartą na wielu silnikach usługę Capture ATP. Mechanizm RTDMI proaktywnie wykrywa i blokuje zagrożenia typu zero-day i nieznany dotąd malware, przeprowadzając kontrolę procesów bezpośrednio w pamięci operacyjnej.

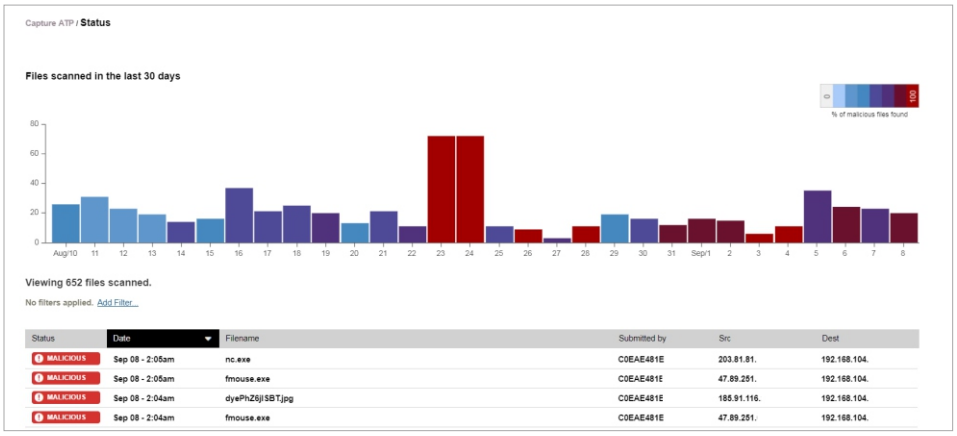
Dzięki architekturze czasu rzeczywistego technologia SonicWall RTDMI działa precyzyjnie, z minimalną liczbą fałszywych wykryć (false positives), identyfikując i neutralizując wyrafinowane ataki.

Analiza wielu typów plików - usługa oferuje analizę szerokiego spektrum rozmiarów i typów plików, w tym programów wykonywalnych, DLL, PDF, dokumentów MS Office, archiwów, JAR i APK oraz wielu systemów operacyjnych, w tym Windows i Android. Administratorzy mogą dostosować ochronę, wybierając lub wykluczając pliki mające być wysłane do chmury w celu analizy - według typu i rozmiaru pliku, nadawcy, odbiorcy lub protokołu. Dodatkowo mogą też manualnie przesyłać pliki do usługi w chmurze.

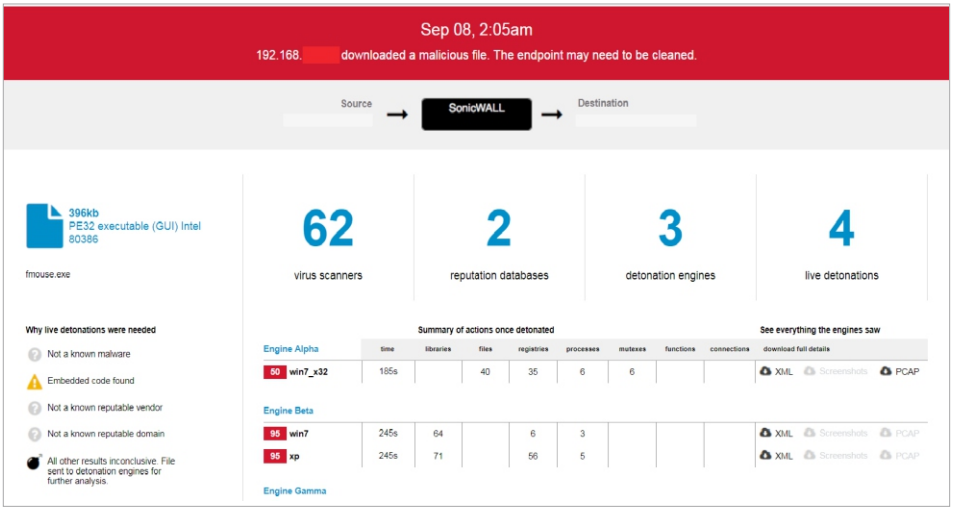
Blokowanie do momentu werdyktu - aby zapobiec przedostawaniu się potencjalnie złośliwego kodu do sieci, pliki wysyłane do usługi w chmurze mogą być zatrzymywane na bramie do momentu uzyskania wyniku analizy.

Szybkie wdrażanie nowych sygnatur - Gdy plik zostanie zidentyfikowany jako złośliwy, firewalle z subskrypcją SonicWall Capture ATP zyskują natychmiastowy dostęp do jego sygnatury, co zapobiega dalszym atakom. Ponadto malware jest przesyłany do zespołu badawczego ds. zagrożeń SonicWall Capture Labs w celu dalszej analizy i dodania informacji o zagrożeniu do baz sygnatur ochrony antywirusowej oraz IPS. Dodatkowo w ciągu 48 godzin informacje są przesyłane do baz danych adresów URL, IP i reputacji domen.

Raportowanie i alerty - usługa SonicWall Capture ATP oferuje konsolę dającą natychmiastowy wgląd w zagrożenia. Udostępnia ona raporty szczegółowo przedstawiające wyniki analiz plików wysyłanych do chmury (w tym źródła, miejsca docelowego i podsumowania z opisem działania szkodliwego oprogramowania po jego uruchomieniu). Rejestry zdarzeń zapory dostarczają powiadomienia o podejrzanych plikach wysłanych do usługi SonicWall Capture ATP oraz zestawienia wyników analizy.



Strona raportowania SonicWall Capture ATP wyświetla całościowe wyniki w ujęciu dziennym. Kolorowe paski w raporcie wskazują dni, w których wykryto złośliwe oprogramowanie. Administratorzy mają możliwość przeklikania poszczególnych wyników dziennych i zastosowania filtrów, w celu szybkiego wglądu w złośliwe pliki i wyniki analiz.



Dostępny jest również szczegółowy raport z analizy złośliwych plików w celu ułatwienia i przyspieszenia działań naprawczych.

Obsługiwane platformy

Usługa SonicWall Capture ATP jest obsługiwana przez następujące firewalle SonicWall z systemem SonicOS 6.2.6 lub nowszym:

NSsp 12800
NSsp 12400

NSa 9650
NSa 9450
NSa 9250
NSa 6650
NSa 5650
NSa 4650
NSa 3650
NSa 2650

TZ600 series
TZ500 series
TZ400 series
TZ350 series
TZ300 series
SOHO 250 series

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

Specjalizowane urządzenia Email Security, programowe oraz hostowane rozwiązanie Email Security (OS 9.0 I nowszy)

WAF Series

SMA 6200, 7200, 8200v (OS 12.0 i nowszy)

SMA 200, 400, 500v (OS 9.1 I nowszy)

Capture Client Advanced

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