



Cisco Umbrella

U prošlosti su sva stolna računala, poslovne aplikacije i kritična infrastruktura bili smješteni iza vatrozida. Danas se sve više događaja događa izvan mreže. Više roaming korisnika. Više korporativnih prijenosnih računala koja pristupaju internetu s drugih mreža. Sve je više aplikacija u oblaku što znači da korisnici ne moraju biti na korporacijskoj mreži kako bi obavili svoj posao. Sve je više poslovnica koje se izravno povezuju s internetom.

Do 2021. Gartner predviđa da će prosječna tvrtka imati 25% svog korporativnog podatkovnog prometa zaobilazeći mrežni perimetar. Kada je korisnik izvan mreže, oni je ranjiv a organizacija nema vidljivost i ne može pružiti adekvatnu zaštitu. Ako se oslanjate samo na sigurnost perimetra, niste u potpunosti zaštićeni. Ovi praznine otvaraju vrata za zlonamjerni softver, otkupnine i ostale napade.

Prva linija obrane

Kao Secure Internet Gateway, Cisco Umbrella pruža prvu liniju obrane protiv prijetnji na Internetu. Umbrella pruža potpuni uvid u sve aktivnosti na svim lokacijama, uređajima i korisnicima te blokira prijetnje prije nego uopće dođu do vaše mreže ili krajnje točke. Kao oblak, Umbrella se jednostavno integrira s vašim postojećim sigurnosnim sustavom i pruža savjete o rješavanju prijetnji.

Analizom i učenjem iz obrasca aktivnosti Interneta, Umbrella automatski otkriva napadačku infrastrukturu postavljenu za napade i proaktivno blokira zlonamjerne zahtjeve prije uspostavljanja veze - bez dodavanja latencije prema korisniku.

Umbrell-om možete pravovremeno spriječiti krađu identiteta i zlonamjerne programe, prepoznati već zaražene uređaja i spriječiti neželjeno curenje podataka.

Provođenje osnovnih pravila interneta

Domain Name System (DNS) je temeljna komponenta Interneta - mapiranje imena domena u IP adrese. Kada kliknete na vezu ili upišete URL, DNS zahtjev pokreće postupak povezivanja bilo kojeg uređaja s internetom. Umbrella koristi DNS kao jedan od glavnih mehanizama za dobivanje prometa na našu platformu za oblak, a zatim ga koristi i za provođenje sigurnosti.

Kada Umbrella-a primi zahtjev za DNS, koristi sofisticirani algoritam da bi utvrdio je li zahtjev siguran, zlonamjerman ili rizičan - što znači da domena sadrži i zlonamjerni i legitimni sadržaj. Sigurni i zlonamjerni zahtjevi usmjeravaju se ili blokiraju. Rizični zahtjevi preusmjeravaju su na proxy poslužitelj na detaljniji pregled. Proxy Umbrella koristi Web tvrtke Cisco Talos i podatke trećih strana kako bi utvrdio je li URL zlonamjerman. Naš proxy također pregledava datoteke koje se pokušavaju preuzeti s tih rizičnih web stranica, pomoću protuvirusnih (AV) uređaja i Cisco Advanced Malware Protection (AMP), i na temelju ishoda ovog pregleda dopuštaju ili blokiraju uspostavu veze.

Benefiti rješenja:

Olakšava troškove sanacije i oštećenja: Obzirom da je Cisco Umbrella prva linija obrane, sigurnosni timovi će imati manje zlonamjernih infekcija za uklanjanje, a prijetnje će biti zaustavljene prije nego što uzrokuju štetu.

Smanjuje vrijeme za otkrivanje prijetnji: Cisco Umbrella sadrži naredbu i kontrolu povratnih poziva preko bilo kojeg priključka ili protokola i pruža izvješća u stvarnom vremenu o toj aktivnosti.

Povećava vidljivost na internetsku aktivnost svih lokacija i korisnika: Cisco Umbrella pruža uvid u incidente i također vam daje uvjerenje da vidite sve.

Identificira aplikacije u oblaku koje se koriste diljem tvrtke: Cisco Umbrella pruža vidljivost u sankcionirane i nesankcionirane usluge u oblaku koje se koriste u cijelom poduzeću, tako da možete otkriti nove usluge, vidjeti tko ih koristi i identificirati potencijalni rizik.



Sofisticirani SW zaustavlja napade prije pokretanja

Globalna mreža Umbrella, tj. mreža na kojoj se temelji rekurzivna DNS usluga, svakodnevno rješava milijarde internetskih zahtjeva milijuna korisnika širom svijeta. Ova velika količinu podataka analizira se u svrhu otkrivanja uzoraka i infrastrukture napadača.

Prikupljamo podatke o aktivnostima iz globalne mreže u stvarnom vremenu u našu masivnu bazu podataka, a zatim primijenjujemo statističke modele u svrhu odbijanja napada. Ove informacije analiziraju stručnjaci koji rade na sofisticiranom SW-u Umbrella, kao što koriste i podatke tvrtke Cisco Talos. Kombinacijom ljudske inteligencije i strojnog učenja identificiramo zlonamjerne web lokacije - bilo da su to domene, IP-ovi ili URL-ovi - diljem Interneta.

Kooperativnost

Umbrella se integrira s vašim postojećim sigurnosnim rješenjem, uključujući sigurnosne uređaje, inteligentne platforme i kontrolne platforme (cloud access security broker, CASB). Umbrella može poslati podatke o aktivnostima vašem SIEM-u (Security Information and Event Management) ili sustavu za upravljanje zapisima (log), i pomoću našeg API-ja, možete slati zlonamjerne domene u Umbrella-u, gdje će biti blokirane. To vam omogućuje da jednostavno proširite zaštitu vašeg sustava.

Implementacija u cijeloj tvrtki za nekoliko minuta

Umbrella je najbrži i najlakši način za zaštitu svih vaših korisnika u nekoliko minuta. Budući da je isporučen iz oblaka, nema hardvera ili softvera koje treba instalirati. Možete opskrbiti sve uređaje na mreži, uključujući BYOD i IoT - za nekoliko minuta i koristiti postojeće Cisco platforme - AnyConnect, Integrirani servisni usmjerivač (ISR) 4K serije i Wireless LAN Controller 5520 i 8540 - kako biste brzo omogućili tisuće izlaza na mrežu i pristupa prijenosnim računalima. Osim toga, pomoću aplikacije Cisco Security Connector možete upotrijebiti proširenje za Umbrella-u kako biste zaštitili iOS 11 uređaje.

Sljedeći koraci

Javite nam se. Razgovarajmo o tome kako Cisco može pomoći u zaštiti vašeg ureda od navedenih prijetnji. Posjetite signup.umbrella.com za besplatnu 14-dnevnu probnu verziju Umbrella-a. Ako vaša organizacija ima 1000 + korisnika, kvalificirana je za [Umbrella Security Report](#), koji pruža detaljnu analizu.

Ključne značajke:

- Vidljivost i zaštita bilo gdje
- Sofisticirani softver za pravovremeno otkrivanje napada ranije
- Jednostavna implementacija i upravljenje
- Otvorena platforma za integraciju
- Brza i pouzdana infrastruktura oblaka

Ključni brojevi:

- 120 milijardi dnevnih internetskih zahtjeva
- 85 milijuna korisnika
- 25 podatkovnih centara dijeljem svijeta
- više od 7 milijuna zlonamjernih odredišta provodi se istodobno u DNS sloju

