PrimeQ En partner. Många specialister.

WEBROOT Smarter Cybersecurity®

Webroot SecureAnywhere® Endpoint Protection

Multi-vector skydd som säkrar endpoints och användare genom alla steg av en cyberattack

Översikt

Moderna hot använder flera vektorer för att attackera, allt från skadliga email med bifogade filer, till infekterade webbannonser som leder till phishing sidor. Brottslingar kombinerar flera olika typer av hot, som sprids i flera olika stadier för att infektera datorer och nätverk. Genom att kombinera flera typer av hot ökar man chansen att lyckas infektera ett nätverk samtidigt som det går snabbare och kan orsaka större skada.

Multi-vector attacker är utformade till att utnyttja svagheter hos signaturbaserade säkerhetssystem och kan enklare infektera nätverk obemärkt. Tyvärr så förlitar sig även moderna system till viss del på signatur-baserade detektions modeller. Den här metoden skyddar enbart användaren efter hotet är känt och en signatur har skapats och uppdaterats till deras endpoint, vilket ofta kan ta för lång tid.

Även nyare, "next-generation" endpoint solutions, som oftast är mer effektiva än deras mer traditionella konkurrenter, är flera gånger inte lika förberedda att bekämpa moderna attacker, då dom enbart skyddar endpoints vid infektionsstadiet och enbart via en enda vektor.

Det enda sättet att stoppa "zero-day" attacker är med multi-vector protection som kan säkra användare och deras enheter vid varje steg av attacken samt genom alla möjliga attack vektorer.

SecureAnywhere® skillnaden

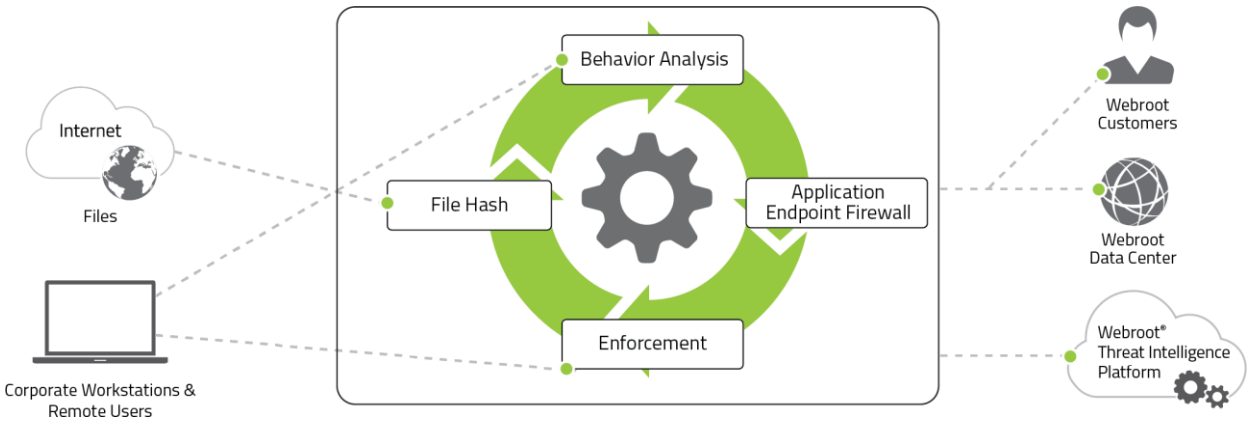
Webroot SecureAnywhere Endpoint protection erbjuder en unik metod som skyddar mot hot genom ett flertal vektorer; inklusive email, web browsing, bifogade filer, hyperlänkar, pop-up reklam, sociala media appar och inkopplade enheter som USB-stickor men även andra typer av kombinerade hot som kan leverera skadliga filer.

Webroots lösningar bygger på den ledande moln-baserad teknologin Webroot Threat Intelligence Platform. I kombination med den senaste real-time intelligensen från Webroot Brightcloud services samt avancerad maskininlärning och beteende baserad hotdetektion, upptäcker, analyserar och klassificerar Webroot hot som varje endpoint upplever i realtid med extremt hög träffsäkerhet.

Genom att kombinera filmönster och beteende kan Webroot med hjälp av industriledande maskininlärning och processkraften från våra molntjänster stoppa zero-day hot samma sekund som dom attackerar. Webroots metod är effektivare och mer pålitlig än dess singel vektor konkurrenter. Du behöver inte längre förlita dig på en utdaterad detektions model som enkelt blir överväldigad av dagens hot – en model som har okända uppehållstider, som inte kan skydda användare förrens efter ett hot redan har infiltrerat ett system och som inte notifierar om en attack förrens långt efter attacken har genomförts.

Eftersom Webroot SecureAnywhere Endpoint Protection är helt molnbaserat, finns det inga definitioner eller signaturer att rulla ut och managera. Hot detektionen sker kontinuerligt i realtid men prestanda är ingenting att oroa sig för. Schemalagda system scanningar tar normal sett runt 18 sekunder och påverkar aldrig enhetens prestanda, även om du kör scanningen på virituella datorer eller i server miljöer. Agenten krockar inte heller med andra antivirus lösningar så det är inga problem att rulla ut Webroot sida vid sida med andra lösningar.

Världens minsta, snabbaste endpoint säkerhets klient erbjuder unikt skydd mot multi-vector hot.



Upptäcker zero-day virus

Synlig Effektivitet

Webroot SecureAnwhere Endpoint Protection är den första lösningen som rapporterar hur effektiv den är på att hitta intrång och stoppa virus. Dwell time reporting ger dig insyn till alla intrång på alla enheter inom ditt nätverk. Webroot visar dig när intrånget skedde och hur lång tid det tog för Webroot att hitta hotet innan det automatiskt åtgärdades.

En stor faktor som bidrar till Webroot SecureAnywhere Endpoint Protections effektivitet är dess kontinuerliga övervakning, journalföring och återställning. Om Webroot inte omedelbart kan kategorisera nya eller förändrade filer och processer som "identifierade bra" eller "identifierade dåliga" kommer agenten börja övervaka och journalföra alla händelser. Om en observerad process blir kategoriserad som skadlig kommer systemet att återställa sig själv till punkten innan processen startades. Det här sista steget försäkrar även oss om ett minimalt antal "false positives". Även om ett false positive uppstår kan admins enkelt vitlista filer som används i deras miljö.

Flexibel Molnbaserad Managering

Webroot SecureAnywhere solutions använder molnbaserad managering. Det betyder att man slipper on-premise hårdvara eller mjukvara samt att konsolen alltid är uppdaterad. Webroots Global Site Management konsol gör det enkelt att managera upp till 100,000 endpoints och genom dess hirarkiska managerings struktur kan du enkelt kontrollera flera kunder och kontor efter företagets behov. Konsolen stödjer även policies på en global och individuel nivå, plus lokala administrations rättigheter och behörigheter som enkelt manageras tillsammans med den centrala administrationen av alla miljöer.

Detta gör Webroots Global Site Manager perfekt för företag av alla storlekar, inklusive globala företag eller företag med kontor över hela landet men även för företag som levererar IT som tjänst till sina kunder. Molnbaserad managering med full fjärradministration gör det även otroligt kostnadseffektivt att leverera global managering jämfört med tradtionellt antivirus.

Infection Dwell Time: Insyn i upptäckt och åtgärd

Förebyggande detektion

Alla Webroot SecureAnywhere lösningar och Brightcloud threat intelligence tjänster drivs av Webroots Threat Intelligence Platform. Genom att använda sig av analyser av big data, maskininlärning och threat intelligence från kunder och teknik partners världen över kan Webroots Threat Intelligence Platform identifiera attacker medans dom pågår. Den samlade datan bearbetas kontinuerligt genom att analysera, korrelera och kontextualisera stora mängder av spridd information samtidigt som en patenterad femte-generations maskininlärning av skadlig kod appliceras och identifierar system för att skapa en förutsägbar beteende igenkäning av skadlig kod.

Genom att processera big data kan Webroot SecureAnywhere Endpoint Protection upptäcka skadlig kod när den försöker infektera en individuell användares endpoint, samtidigt som den skyddar alla andra endpoints mot samma attack. Den här kollektiva strategin till threat intelligence skapar ett massivt real-tids hot detektions nät som har information om mer än 300 miljoner program, inklusive exekveringsmönster och hur de interagerar med systemet. Det här tillsammans med hundratals terrabite av hot data, försäkrar att Webroot kunder är konstant skyddade mot dagens och framtidens hot.

Säkerhetet i Webroot

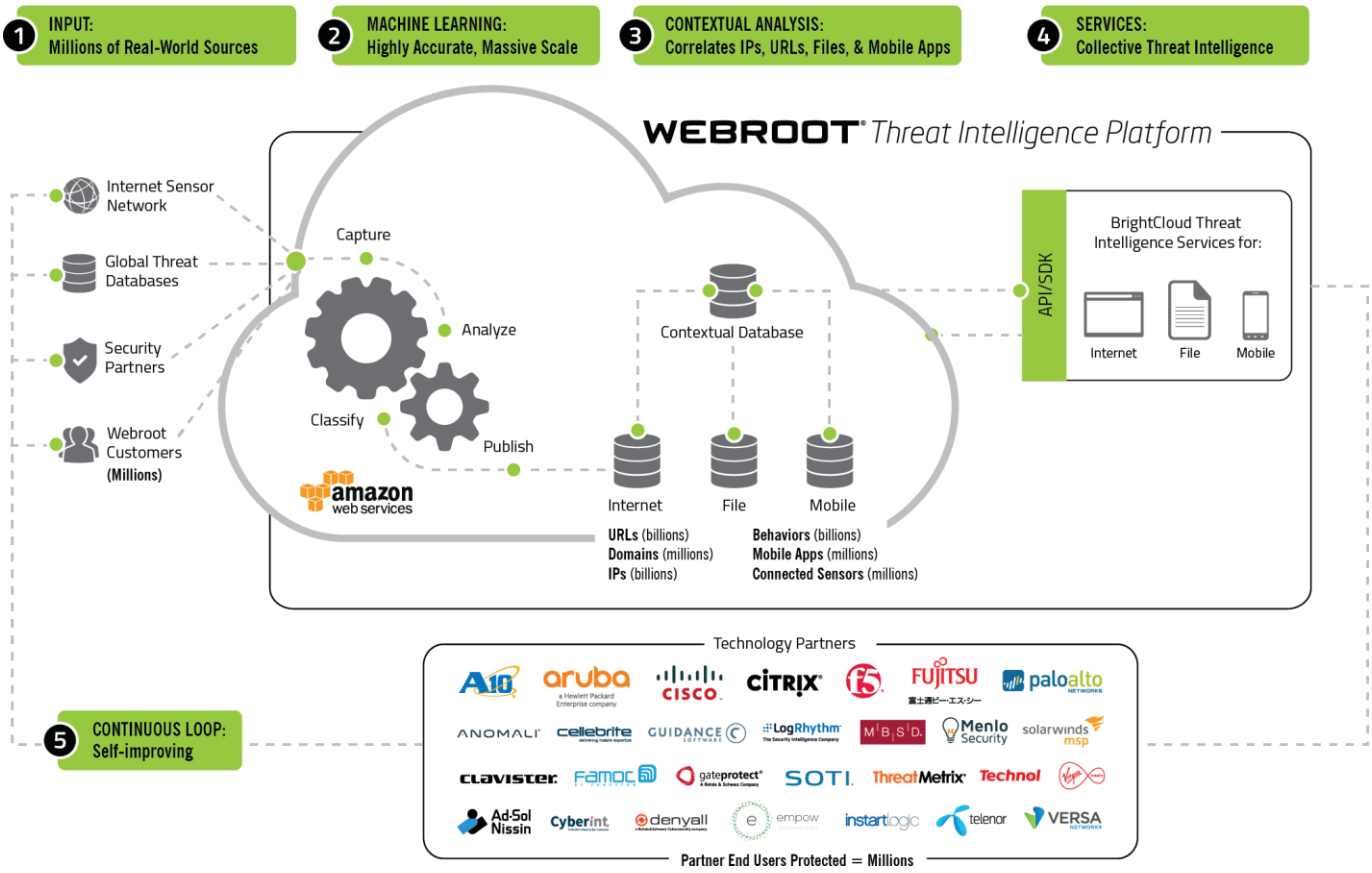
Webroot SecureAnywhere Endpoint Protection erbjuder hög säkerhet och ett effektivt skydd mot skadlig kod med flera lager av säkerhet för att skydda både användare och enheter.

Identity Shield

Den här sköldern skyddar användarna genom att anta att deras endpoint redan är infekterad av hot som inte har upptäckts än. Den skyddar användar- och transaktionsdata som kan vara exponerat under nättransaktioner av phishing, DNS poisining, keylogging, screen grabbing, cookie scraping, clipboard grabbing samt webbläsar och sessions kapning av skadlig programvara som installerar man-in-the-middle attacker. Sköldarna låser operativsystemet och webbläsaren för att skydda all användarinformation. Bortsett från att säkra aktiviteter i webläsaren, så kan Webroots Identity Shield utökas under användar policien till att säkra andra applikationer också.

Infrared

Infrared är ett skydd med flera lager som integrerar flera aspekter av Webroot Threat Intelligence för att hindra hot tidigt i deras livscykel – ofta innan ett hotet har setts till. Det undersöker vilket rykte hemsidorna som en individ besöker har och använder Webroot Threat Intelligence för att bedöma deras risk nivå. Om användaren ofta besöker hemsidor med ett dåligt



Webroot® Threat Intelligence Platform – den mest kraftfulla real tids hot analys motorn I världen

rykte så kommer agenten gå in i ett tillstånd av ökad uppmärksamhet och noggrant undersöka nya filer eller processer som introduceras till systemet. Infrared tolkar också användarens beteende och deras generella säkerhetsnivå. Om en användare klassas som "hög risk" kommer Webroot att dynamiskt anpassa hur den stoppar hot efter användaren medans Webroot fortfarande stoppar false positivies för mindre riskabla användare.

Web Threat Shield

Web Threat skölden utnyttjar Webroots anti-phishing teknologi för att erbjuda ett unikt realtids skydd mot polymorfiska phising URL:er, men även skadliga och "hög-risk" hemsidor och domäner.

Intelligent Outbound Firewall

Som ett tillägg till sina sköldar inkluderar Webroot Secure Anywhere en intelligent systemövervakning och applikationsmedveten utgående brandvägg som förstärker Microsoft Windows® brandvägg för att skydda användare på och frånvarande från företagets nätverk. Det övervakar all utgående trafik för att skydda mot "phone-home", den tillåter endast godkända program att kommunicera med nätverket och känner automatiskt igen kända bra och kända dåliga program. Användarna störs inte med pop-ups eller tvingas göra oinformerade bedömningar.

Powerful Heuristics

Heuristik inställningar kan anpassas baserat på risken för fil exekvering. Heuristik inställningarna inkluderar:

» **Avancerade**
Analyserar nya program för misstänkt beteende som är typiskt för skadlig kod

» **Ålder**
Analyserar nya program baserat på den tiden en liknande fil har existerat inom Webroot Threat Intellience

» **Populäritet**
Analyserar nya program baserat på hur ofta en fil används eller ändras inom Webroot Threat Intelligence

Offline Skydd

Stoppar attacker när en endpoint är offline med separat fil exekverings policies som kan applicerat till lokal hårddisk, USB, CD och DVD enheter.

Virtualization, Terminal Server & Citrix Support

Utöver Windows PC miljöer stödjer Webroot Secure Anywhere Endpoint Protection även Windows Servrar, Viritualisering, Terminal servrar och Citrix miljöer.

Resilient Distributed Cloud Architecture

Består av flera säkra globala data center för att stödja lokala kontor och resande användare med hållbarhet och redundans genom deras närmaste datacenter

Om Webroot

Webroot levererar nästa generations nätverk och endpoint säkerhet samt threat intelligence tjänster för att skydda, företag och individer över hela världen. Vår smartare inställning utnyttjar kraften av cloudbaserad kollektiv threat intelligence kommer från miljoner av verkliga enheter för att kunna stoppa hot i realtid och hjälpa till att säkra en uppkopplad värld. Våra prisbelönta SecureAnywhere Endpoint lösningar och BrightCloud Threat Intelligence tjänster skyddar miljoner enheter genom flera olika branscher, hem användare och Internet of Things. Integrerad och betrodd av marknadsledande företag, inklusive Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, med flera. Webroots huvudkontor ligger i Kolorado och arbetar globalt genom Nord Amerika, Europa och Asien. Upptäck smartare Cybersecurity lösningar på webroot.com

World Huvudkontor
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900